

# Universal Desktop Linux v5

User Manual



**IGEL**<sup>®</sup>  
**UNIVERSAL  
DESKTOP**

# Important Information

Please note some important information before reading this documentation.

## Copyright

This publication is protected under international copyright laws. All rights reserved. With the exception of documentation kept by the purchaser for backup purposes, no part of this manual – including the products and software described in it – may be reproduced, manipulated, transmitted, transcribed, copied, stored in a data retrieval system or translated in any form or by any means without the express written permission of IGEL Technology GmbH.

Copyright © 2015 IGEL Technology GmbH. All rights reserved.

## Trademarks

IGEL is a registered trademark of IGEL Technology GmbH.

Any other names or products mentioned in this manual may be registered trademarks of the associated companies or protected by copyright through these companies. They are mentioned solely for explanatory or identification purposes, and to the advantage of the owner.

## Disclaimer

The specifications and information contained in this manual are intended for information use only, are subject to change at any time without notice and should not be construed as constituting a commitment or obligation on the part of IGEL Technology GmbH. IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including any pertaining to the products and software described in it. IGEL Technology GmbH makes no representations or warranties with respect to the contents thereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

## IGEL Support and Knowledge Base

If you have any questions regarding an IGEL product and are already an IGEL customer, please contact your dedicated sales partner first. Er beantwortet gerne Ihre Fragen rund um alle IGEL-Produkte.

If you are currently testing IGEL products or your sales partner is unable to provide the help you need, please fill in the support form after logging on at the <http://www.igel.com/de/mitgliederbereich/anmelden-abmelden.html>.

We will then contact you as soon as possible. It will make things easier for our support staff if you provide us with all the information that is available. Please see also our notes regarding support and service information. Please visit our *IGEL Knowledge Base* <http://edocs.igel.com/> to find additional Best Practice and How To documentation as well as the *IGEL Support-FAQ* (<http://faq.igel.com>).

# Contents

Important Information .....	2
1. Introduction .....	9
1.1. Supported formats and codecs .....	9
2. Quick Installation .....	11
2.1. The IGEL Linux desktop .....	12
3. Boot Procedure .....	13
3.1. Boot Menu .....	13
3.2. Network Integration .....	15
3.3. X-Server .....	15
4. Application Launcher .....	15
4.1. General System Information .....	16
4.2. Sessions .....	16
4.3. System Tools .....	17
4.4. License .....	18
4.5. Network Information .....	18
4.6. Shutdown and Restart .....	19
5. Setup Application .....	19
5.1. Starting the Setup .....	19
5.2. Completing the Setup .....	19
5.3. Setup Areas .....	20
5.4. Enable setup pages for users .....	21
5.5. Quick setup .....	22
5.6. Setup Search .....	22
6. Sessions .....	23
6.1. Desktop integration .....	23
6.2. Citrix Receiver selection .....	24
6.3. Citrix ICA - global settings .....	24
6.4. Citrix ICA - Sessions .....	35
6.5. Citrix StoreFront / Web Interface .....	39
6.6. Citrix Access Gateway .....	42
6.7. RDP - global settings .....	42
6.8. RDP session .....	50
6.9. Remote desktop web access .....	53
6.10. Horizon Client Global .....	58
6.11. Horizon Client sessions .....	62
6.12. Quest vWorkspace Client and AppPortal .....	65
6.13. Appliance mode .....	66
6.14. Leostream Connection Broker .....	69
6.15. Systancia AppliDis Client .....	69
6.16. Evidian AuthMgr .....	69

6.17.	NoMachine NX .....	70
6.18.	X Session .....	70
6.19.	Parallels 2X client session .....	70
6.20.	PowerTerm WebConnect.....	71
6.21.	PowerTerm terminal emulation.....	71
6.22.	IBM iSeries Access.....	72
6.23.	ThinLinc .....	73
6.24.	SSH Session .....	77
6.25.	VNC Viewer .....	78
6.26.	VERDE session .....	78
6.27.	Firefox browser .....	79
6.28.	Media Player .....	94
6.29.	Java Web Start Session .....	97
6.30.	VoIP Client.....	97
7.	Accessories .....	98
7.1.	ICA Connection Center.....	98
7.2.	Local Terminal .....	98
7.3.	Change Smartcard Password .....	98
7.4.	Setup Session .....	98
7.5.	Quick Settings Session.....	99
7.6.	Display switch .....	99
7.7.	Application Launcher .....	102
7.8.	Sound Mixer.....	102
7.9.	System Log Viewer .....	102
7.10.	UMS Registration .....	103
7.11.	Touchscreen calibration.....	104
7.12.	Task Manager.....	104
7.13.	Screenshot tool .....	106
7.14.	Soft keyboard.....	108
7.15.	Java Manager .....	109
7.16.	Monitor Calibration.....	109
7.17.	Commands .....	109
7.18.	Network Diagnostics .....	109
7.19.	System Information.....	111
7.20.	Disk Utility .....	111
7.21.	Firmware Update .....	112
7.22.	Smartcard Personalization .....	112
7.23.	Identify Monitors .....	113
7.24.	Upgrade License.....	113
7.25.	Webcam Information.....	114
7.26.	Image viewer.....	115
8.	User Interface .....	116
8.1.	Screen.....	116
8.2.	Desktop .....	124
8.3.	Language .....	131

8.4.	Screen Saver and Screen Lock.....	131
8.5.	Input .....	134
8.6.	Hotkeys .....	140
8.7.	Font Services .....	141
9.	Network .....	143
9.1.	LAN interfaces .....	143
9.2.	Proxy .....	160
10.	Devices .....	161
10.1.	Printers.....	161
10.2.	USB Storage Devices .....	165
10.3.	Smartcard.....	167
10.4.	USB access control .....	167
11.	Security.....	169
11.1.	Password.....	169
11.2.	Login Options .....	170
11.3.	AD/Kerberos Configuration.....	174
12.	System Settings .....	175
12.1.	Time and Date .....	175
12.2.	Update.....	176
12.3.	Remote management .....	177
12.4.	Buddy Update .....	179
12.5.	Shadow.....	179
12.6.	Remote Access (SSH / RSH).....	183
	Power .....	183
12.7.	Firmware Customization.....	188
12.8.	IGEL System Registry.....	199
13.	Index .....	200

## About this Manual

All illustrations and descriptions in this manual relate to Version 5.08.100 of the IGEL Linux firmware.

This manual is divided into the following sections:

<b>Introduction</b>	General information about the product
<b><i>Quick installation</i> (page 11)</b>	Setting up the thin client for the first time
<b><i>Boot procedure</i> (page 13)</b>	Boot menu, network integration, X-Server
<b>Application Launcher</b>	Important system data such as the firmware version, list of applications, licensed services, system tools
<b><i>Setup application</i> (page 19)</b>	Setting up sessions and system configuration
<b><i>System settings</i> (page 175)</b>	System setting options
<b><i>User interface</i> (page 116)</b>	Language, screen, entry options, font services
<b><i>Network</i> (page 143)</b>	Interfaces, protocols, authentication, drives
<b><i>Sessions</i> (page 23)</b>	Creating and configuring application sessions
<b><i>Accessories</i> (page 98)</b>	Session accessories, card readers, sound control, Java Manager, network diagnostics
<b><i>Devices</i> (page 160)</b>	Hardware, printers, storage devices, interfaces
<b><i>Security</i> (page 169)</b>	Password, logging on, AD/Kerberos configuration
<b><i>IGEL smartcard</i> (page 170)</b>	Company keys, saving a user/password/session, testing a card
<b><i>Firmware configuration</i> (page 188)</b>	Customer-specific partition, applications, commands, start screen, environment variables, features

## Formatting and Meanings

The following formatting is used in this document:

<b><i>Hyperlink</i></b>	Internal or external links
<b>Proper names</b>	Proper names of products, companies etc.
<b>GUI text</b>	Items of text from the user interface
<b>Menu &gt; Path</b>	(Context) menu paths in system and programs
<b>Input</b>	Program code or system input
<b><span style="border: 1px solid black; padding: 0 2px;">Key</span></b>	Commands entered using keys



A note regarding operation



**Warning:** Important note which must be observed.



A reference to other manual topics or to documents on eDocs.

## What is new in 5.08.100?

You will find the release notes for IGEL Linux 5.08.100 as a text file alongside the installation programs on our download server and in our Knowledge Base eDocs. New Features:

- **Dynamic drive mapping for RDP sessions:**  
A USB mass storage medium will automatically be removed from the RDP session when it is disconnected from the device. Further information can be found under *Hotplug Storage Devices* (page 165).
- **Preset permissions for hotplug storage devices:**  
The permissions for hotplug storage media can be preset. Further information can be found under *Hotplug Storage Devices* (page 165).
- **Quick setup can be brought up in appliance mode:**  
Using a hotkey, the quick setup can be brought up in the appliance mode. Further information can be found under *Quick Setup* (page 21).
- **Window size can be changed during an RDP session:**  
In RDP sessions the window size can be changed while the session is running. Further information can be found under *Window – RDP* (page 44).
- **Display filter expanded in Citrix StoreFront:**  
The display filter for applications in Citrix StoreFront / Web Interface can also be applied to the Application Launcher. Further information can be found under *Appearance* (page 40).
- **New Task Manager application:**  
The firmware now provides a task manager. Further information can be found under *Using the Task Manager* (page 105) and *Task Manager* (page 104).
- **Configurable vertical taskbar:**  
The way in which labels are displayed can be configured; the arrangement of the symbols has been optimized. Further information can be found under *Taskbar* (page 126).
- **Intelligent taskbar:**  
The taskbar can be configured so that it is automatically hidden if the display area is needed. Further information can be found under *Taskbar* (page 126).
- **Network Level Authentication (NLA) available for VMware Horizon:**  
Network Level Authentication (NLA) can be used for VMware Horizon sessions based on RDP. Further information can be found under *Options* (page 64).

- Presets for VMware Horizon are carried over from RDP presets:

The global presets for drive mapping for RDP sessions also apply to VMware Horizon sessions, even if PCoIP is used. Further information can be found under *Horizon Client Global* (page 58).

- Firmware Customization has been optimized:

Firmware Customization is now easier thanks to a new *Corporate Design* (page 195) area in the setup.

- New display zoom function:

With the new *display zoom* (page 101) function, you can magnify the setup interface on the screen.

- New Screenshot Tool:

The firmware now includes a screenshot tool. Further information can be found under *Taking a Screenshot* (page 107) and *Screenshot Tool* (page 106).

- Defining computer name for UMS registration:

During UMS registration, you can now specify a *custom name for your client* (page 177).

- The touchscreen configuration has been expanded.



# 1. Introduction

IGEL Thin Clients comprise the very latest hardware and an embedded operating system. Depending on the product concerned, this operating system may be based on IGEL Linux or Microsoft Windows Embedded Standard\*. We have done our utmost to provide you with an excellent overall solution and promise to provide the very same level of quality service and support.

The firmware included with every IGEL Universal Desktop product is multi-functional and contains a wide range of protocols allowing access to server-based services. The IGEL Universal Desktop Firmware is available with two possible operating systems and with the following options:

Operating system	Options
Windows Embedded Standard 7	<ul style="list-style-type: none"><li>• Ericom PowerTerm Terminalemulation</li><li>• IGEL Shared Workplace</li><li>• IGEL Universal MultiDisplay (LX only)</li><li>• Codec package (LX only)</li></ul>
IGEL Linux	

The structure of the IGEL setup is almost identical on all thin clients and in the Universal Management Suite (UMS) management software. This means that the configuration parameters in the local device setup can be found in the same location in the tree structure as a profile used in the management software for example.

The IGEL Universal Management Suite is available to all customers on the IGEL download site. It allows management of an unlimited number of IGEL thin clients.

## 1.1. Supported formats and codecs

IGEL Linux supports the following multimedia formats and codecs out of the box:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC

The following codecs are licensed via the separately available Multimedia Codec Pack:

Supported formats:	Supported codecs:
AVI MPEG ASF (restricted under Linux) WMA WMV (restricted under Linux) MP3 OGG	MP3 WMA stereo WMV 7/8/9 MPEG 1/2 MPEG4 H.264



AC3 is not licensed.



IGEL Zero Clients (IZ series) have the Multimedia Codec Pack installed by default.

## 2. Quick Installation

If you follow the procedure below, you can install the thin client within your network environment in just a few minutes:

1. Connect the thin client to a monitor (VGA, DVI, DisplayPort), an AT-compatible keyboard with a PS/2 or USB connection, a USB mouse and the LAN using an RJ45 connector.
2. Connect the thin client to the power supply.
3. Start the thin client and wait until the graphical user interface has loaded.
4. Click on the **Setup** symbol in the taskbar, or launch the IGEL Setup using the key combination **Ctrl+Alt+S**.
5. Select the system language and keyboard layout under **User Interface > Language**.
6. Select the display resolution under **User Interface > Display**.
7. Enter a local IP address in the **Network** section of the setup or retain the default DHCP mode for automatic network configuration.
8. Click on **OK** to save and apply your changes.

The device will now restart if necessary and will use the new settings thereafter.



A handy tool tip is available for virtually every setting. If you would like to know more about a setting or option, move your mouse pointer over it and wait for a moment. You can configure the tool tips under **User Interface > Screen > Desktop**.

## 2.1. The IGEL Linux desktop

After the system starts, you will see the IGEL Linux desktop.



Figure 1: IGEL Linux desktop

The following components can be found in the taskbar at the bottom edge of the screen:

- **Start menu** (also IGEL menu)
- **Quick launch bar** with symbols for the **Application Launcher**, **setup** and sessions
- **Info area** with symbols for the **volume**, **network**, **time** and **desktop** (show/hide window)

The Start menu offers the following areas and functions:

- **Application area** for launching sessions
- **System area** for access to system programs
- **Info area (About)** for displaying all relevant system information
- **Search** for finding functions in the Start menu
- Buttons for **shutting down** and **restarting** the system

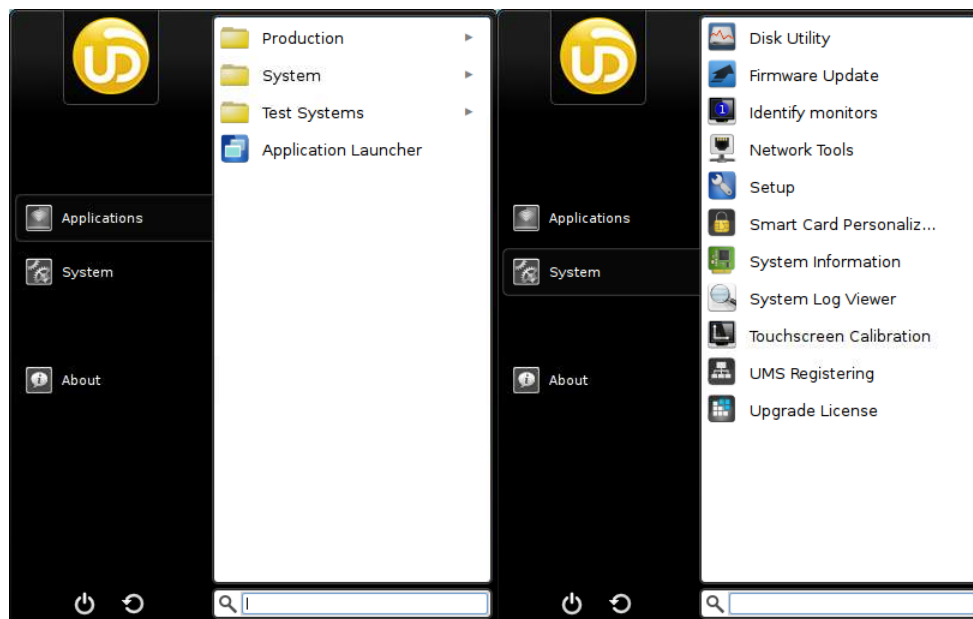


Figure 2: IGEL Start menu with application and system area

## 3. Boot Procedure

The quick installation procedure is complete.

- Restart the system in order to start the boot procedure.

### 3.1. Boot Menu

- During the boot procedure, press the **ESC** key in the **Secondstage Loader** when the **Loading Kernel** message is shown on the screen.

A menu with four boot options as well as an option for resetting the thin client to the default factory settings will appear:

- **Quiet Boot (page 14):** Normal boot
- **Verbose Boot (page 14):** Boot with system messages
- **Emergency Boot (page 14):** Setup only
- **Failsafe Boot (page 14):** With CRC check
- **Reset to Factory Defaults (page 14):** Resets the thin client to the default factory settings

### 3.1.1. Quiet Boot

**Quiet Boot** is the default boot mode. In this mode, all kernel messages are disabled and the graphical user interface is started.

### 3.1.2. Verbose Boot

Unlike in **Quiet Boot** mode, the boot messages are shown in **Verbose Boot** mode. A diagnostics shell is also available. This can be used to execute common commands (such as `ifconfig` etc.) when searching for and rectifying faults.

➤ Enter `init 3` to close this shell.

The boot procedure will then resume.

### 3.1.3. Emergency Boot

**Emergency Boot** is a setup with default parameters.

If you select **Emergency Boot**, the Secondstage Loader looks for a bootable system in the flash memory and then resumes the boot procedure as in the other boot modes.

Essentially speaking, the X-Server is started without network drivers and with a resolution of 1024 x 768 - 60 Hz during an **Emergency Boot**. The **Setup** menu is then opened directly.

This option is useful if, for example, you have selected an excessively high screen resolution or a wrong mouse type and these settings can no longer be changed in the normal setup.

### 3.1.4. Failsafe Boot - CRC check

During a **Failsafe Boot**, a check of the file system is carried out first. The thin client then starts in **Verbose Mode**.

### 3.1.5. Reset to Factory Defaults

If you select **Reset to Factory Defaults**, all personal settings on the thin client (including your password and the sessions you have configured) will be lost.

A warning message will appear on the screen before the procedure is carried out.

➤ You must then confirm your decision.

If the device is protected by an administrator password, you will be prompted to enter this password. You have three attempts to do so.

Do you not know the password?

1. When you are prompted to enter the password, press the Enter key three times.
2. Press C to bring up the **Terminal Key**, the individual key for the thin client.
3. Contact us using an RMA form:

➡ <https://www.igel.com/en/service-support/rma-request.html>

1. Enter the **Terminal Key** shown, the firmware version and your contact details.

Our service department will send you a so-called Reset to Factory Defaults Key specially for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.

➡ See also the FAQ Resetting a Thin Client with unknown Administrator Password.

## 3.2. Network Integration

Is the kernel loaded?

If it is, the next step is the network configuration.

There are three possible ways of integrating the terminal into the network environment. Depending on the terminal's settings, you can choose between **DHCP**, **BOOTP** or a **manually configured IP address**.

## 3.3. X-Server

The final step in the boot procedure involves starting the X-Server and the local window manager.

# 4. Application Launcher

- To launch the tool, click on the **Application Launcher** symbol in the quick launch bar or in the Start menu.

The various Launcher sub-areas allow access to configured sessions/system programs or show information relating to licenses, the system and network connections.

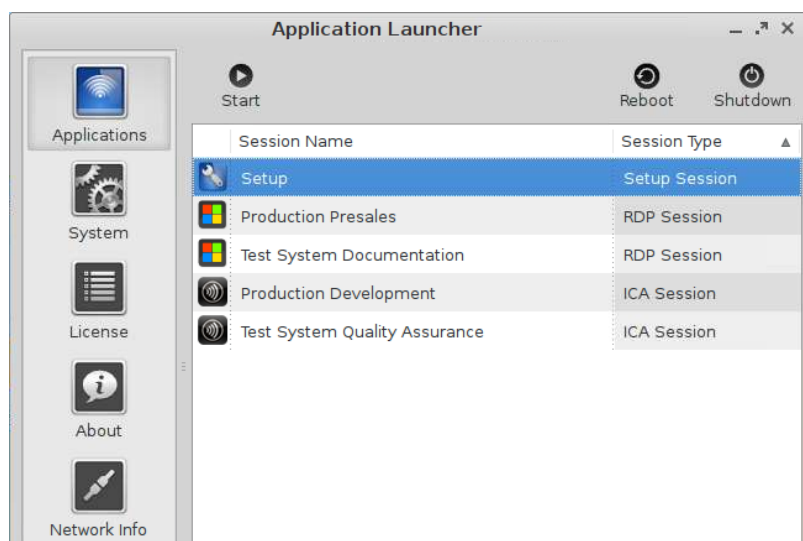


Figure 3: Application Launcher

Because the setup program is the central configuration tool for all thin client settings, a setup session is already pre-defined under **Sessions** and **System**.

## 4.1. General System Information

Within the **Application Launcher** you will find the **Information** page with important system data such as the firmware version, licensed services and hardware specifications.

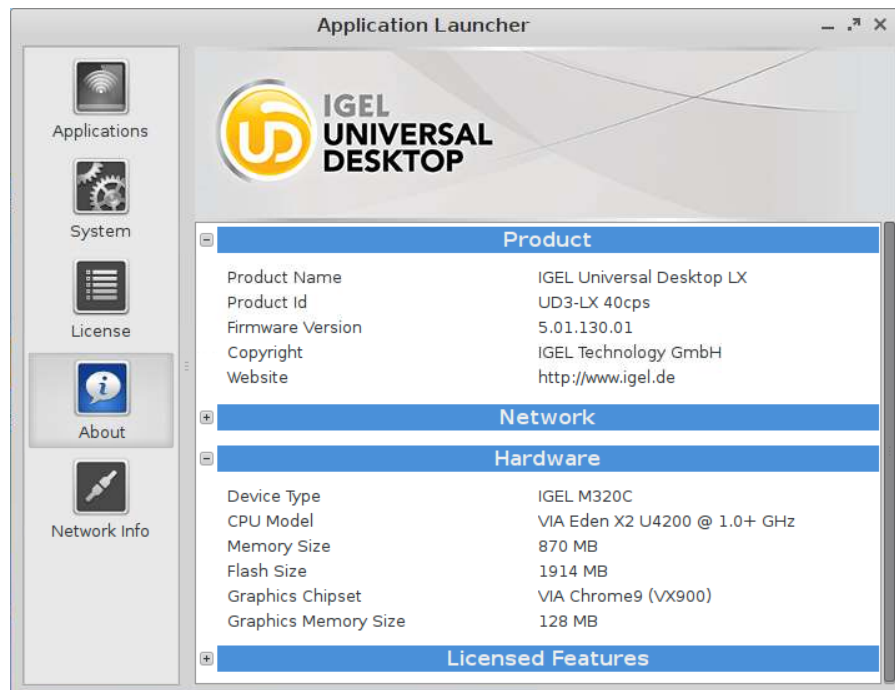


Figure 4: Application Launcher - system information

Details of the current network configuration with the IP address and device name are also given here.

## 4.2. Sessions

All sessions created are shown in a list of applications if they are enabled for the main session page.

- To open an application, double-click on it or click on **Run**.
- Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu.
- Applications can also be launched automatically and a key combination (hotkey) can be defined.



The available options for launching a session can be defined under **Desktop Integration** in the session configuration.



## 4.3. System Tools

On the **System** page, you can run various tools including the firmware updating tool with the pre-set update information.



Figure 5: Application Launcher - system tools

The following tools are available:

Identify monitors	Shows the screen's number and manufacturer details.
Firmware update	Carries out the update with the settings made during the setup.
Disk utility	Shows information regarding connected USB drives.
Upgrade license	Reads a new license file from the USB stick and modifies the functions of the firmware accordingly.
Network tools	Provides detailed information on the network connection and offers a number of problem analysis tools such as Ping or Traceroute.
Setup	Launches the IGEL Setup.
Smart Card personalization	Allows access data and sessions which are to be available to a smartcard user to be written to an IGEL smartcard.
System information	Shows information regarding hardware, the network and connected devices.
System log viewer	Shows system log files "live" and allows you to add your own logs.
Touchscreen calibration	Allows a connected touchscreen monitor to be calibrated.
UMS registering	Logs the thin client on to a UMS server (access data for the server are required).
Webcam Information	Shows video data of a detected webcam and allows to test the cam.

## 4.4. License

You will find the following here:

- The licenses for the components used in the UD system
- Information on the provision of source code, e.g. under GPL

## 4.5. Network Information

The **Network information** tool allows you to read out data from your local network connections and check the availability of a UMS server:

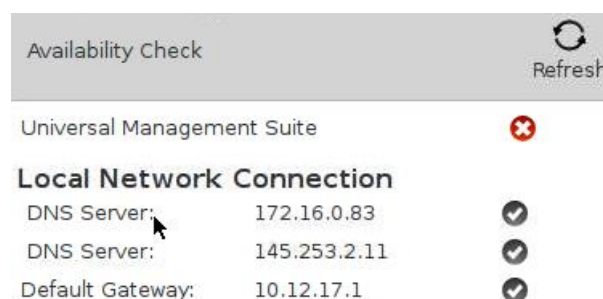


Figure 6: Network information

## 4.6. Shutdown and Restart

Within the **Application Launcher** you will find two buttons for starting or shutting down the device. Both actions can be disabled for the user and will then be available to the administrator only.

You can change the standard action when shutting down the device using the button on the screen or the on/off button on the device itself in the setup under **System→Energy→Shut Down**.

## 5. Setup Application

With the help of the setup, you can change the system configuration and session settings.



Any changes you have made in UMS take precedence and may no longer be modifiable. A lock symbol before a setting indicates that it cannot be changed.

### 5.1. Starting the Setup

You can open the setup in the following ways:

- Double-click on **Setup** in the **Application Launcher** or click on **Run**.
- Double-click on **Setup** on the desktop (if available based on the settings).
- Select **Setup** in the context menu on the desktop (if available based on the settings).
- Select **System→Setup** in the Start menu.
- Click on **Setup** in the quick launch bar.
- Launch the setup using the keyboard command **Ctrl+Alt+S**, or in the Appliance mode using **Ctrl+Alt+F2**.



You can configure how the setup can be launched under **Accessories**. The options described above as well as combinations thereof are available.

### 5.2. Completing the Setup

The buttons **OK**, **Cancel** and **Apply** are usually available on every individual setup page.

- Click on **Apply** if you have finished configuring a setup area and would like to save your settings without closing the setup program.
- Click on **Cancel** if you have not made any changes and would like to abort the setup.

- Click on **OK** to save your changes and exit the setup.

## 5.3. Setup Areas

The setup application comprises the following main areas:

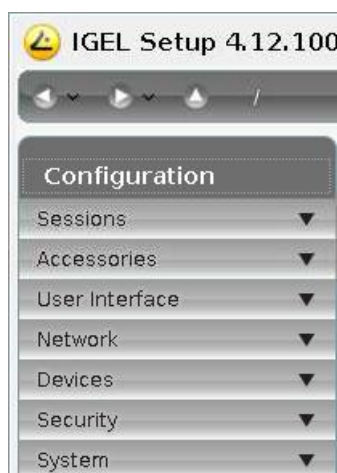


Figure 7: Setup areas

Sessions	Allows you to configure application sessions such as ICA, RDP, PowerTerm, browser and others
Accessories	Allows you to configure various local tools - setup pages for the local shell (Terminal), sound mixer, screen keyboard (for touchscreen monitors), options for the <b>Application Launcher</b> and the setup application itself.
User interface	Allows you to configure display settings, entry devices, hotkey commands etc.
Network	Allows you to configure all network settings for LAN/WLAN interfaces and the dial-up connections
Devices	Allows you to configure various devices
Security	Allows you to set the administrator/user passwords and user authorizations etc.
System	Allows you to set various basic system parameters including the date and time, information regarding the firmware update, remote management etc.

- Click on one of the areas to open up the relevant sub-structure.

The tree structure allows you to switch between the setup options.

Three navigation buttons are available. The buttons allow you to move back and forth between the setup pages you have visited or reach the next level up within the structure.

You will find a more detailed description of the individual setup options elsewhere. This is merely a brief overview.

## 5.4. Enable setup pages for users

If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e. after entering the password (see *Password* (page 169)). However, individual areas of the setup can be enabled for the user, e.g. to allow them to change the system language or configure a left-handed mouse.

To enable setup pages for the user, proceed as follows:

1. Under **Security > Password**, enable the password for the **administrator** and the **setup user**.



If users are to be allowed to edit parts of the setup even without a password, create a quick setup session, the password for the **setup user** will not be enabled in this case.

2. Under **Accessories > Setup > User Page Permissions**, enable those areas to which the user is to have access.
  - A check in the checkbox indicates that the node is visible in the setup.
  - A green symbol (open lock) indicates that the user is able to edit the parameters on this setup page.

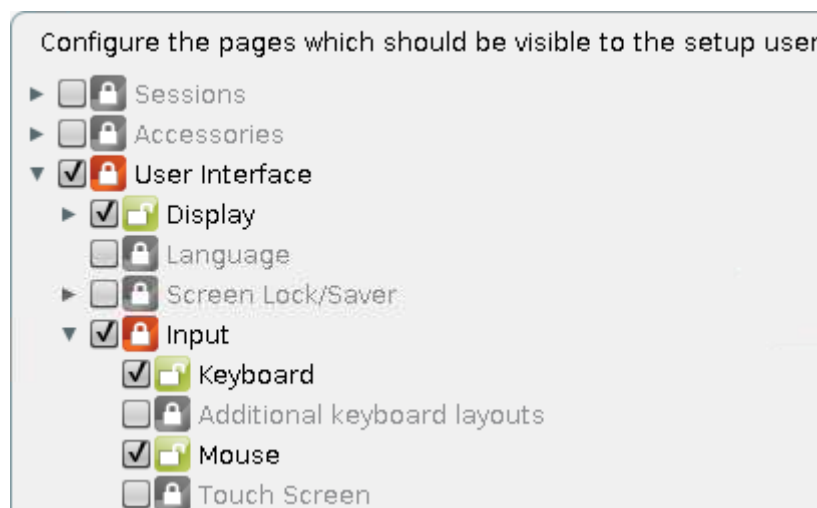


Figure 8: Restricted access to the setup



If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

## 5.5. Quick setup

To create a quick setup session, proceed as follows:

1. Under **Setup > Security > Password**, enable the password for the administrator.



If users are to be allowed to edit parts of the setup only with a password, enable the password for the setup user too.

2. Under **Setup > Accessories > Quick Setup**, define the name and the options for bringing up the quick setup.
3. Under **Setup > Accessories > Quick Setup > User Page Permissions**, enable those areas to which the user is to have access.



You can set up a hotkey in order to launch quick setup in the appliance mode. You will find instructions for setting up the hotkey under *Desktop Integration* (page 23).

## 5.6. Setup Search

The **Search** function enables you to find parameter fields or values within the setup.

1. To start a search, click on the button below the tree structure.
2. Enter the text you wish to search for.
3. Specify the details for your search – narrow it down to field headers for example.
4. Select one of the hits.
5. Click on **Show Result** and you will be taken to the relevant setup page.

The parameter or value found will be highlighted as shown below.

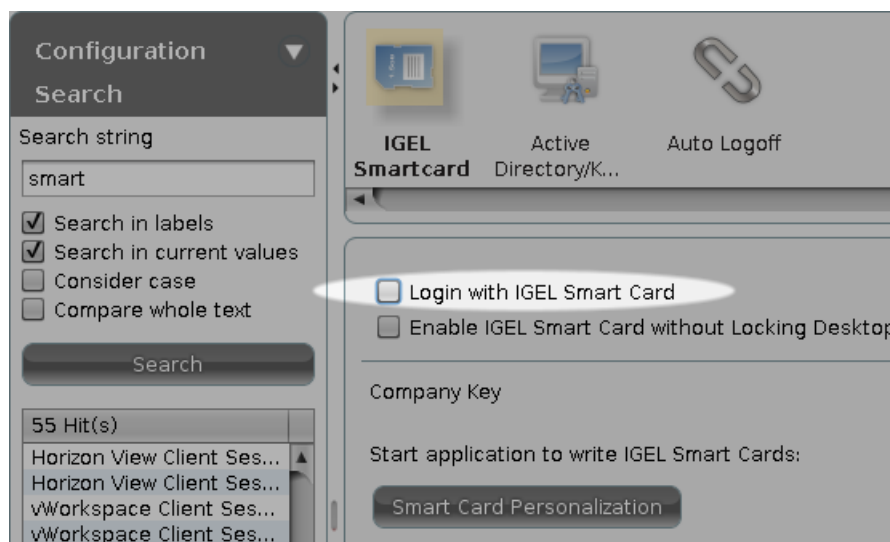


Figure 9: Setup search

## 6. Sessions

Application sessions can be created and configured in the **Sessions** sub-structure of the IGEL setup application. The **Session Overview** provides an overview of all available session types and existing sessions.

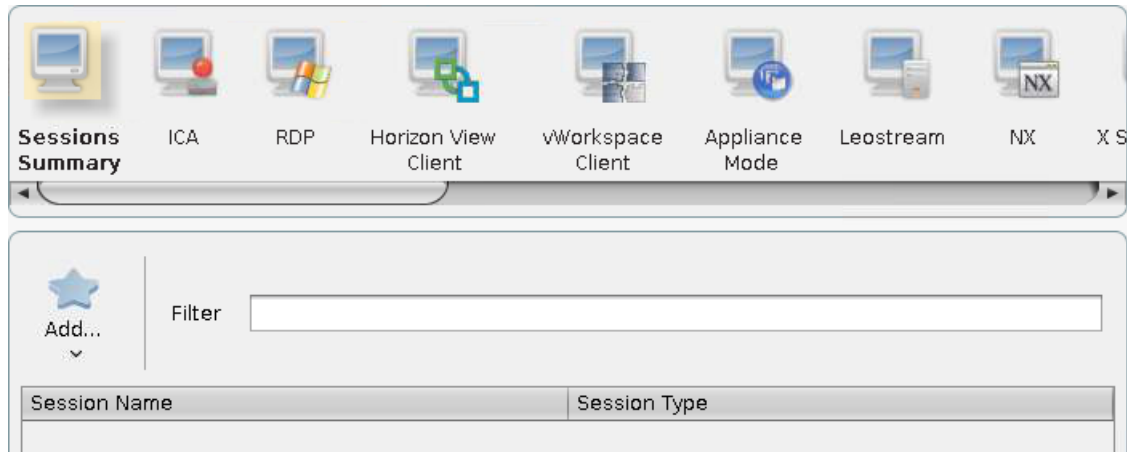



Figure 10: Session overview

- Click on **Add** to create a new session.  
Disabled services are not shown in the drop-down list.

### 6.1. Desktop integration

For each session, there is a **desktop integration** configuration page on which the following actions can be performed:

- Determining the **appearance** of the session on the local desktop.
- Setting up the **name** of the session.

	<p>The session name must not contain any of these characters:</p> <p>\ / : * ? " &lt; &gt;   [ ] { } ( )</p>
---	--

- Selecting the **session start options** (autostart, restart).
- Enabling **hotkey** use.
- Setting a **password for launching the session** (administrator, user, setup user).

If the **Use hotkey** option is enabled, you can log off from a session using a key combination. The combination consists of **modifiers** such as **Ctrl** (Control), **Alt** and **Shift** and a number or a letter as a **key**.

## 6.2. Citrix Receiver selection

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix Receiver Selection**

Select which of the installed Citrix Receiver versions is to be used for Citrix sessions:

- **Standard**
- **12.1.8**
- **13.1.4**
- **13.2.1**



The preset **Standard** setting now corresponds to Citrix Receiver 13.2.1. Previously, Version 12 was preset.



After changing the Receiver version, check

- the settings for the StoreFront / Web Interface server under **Citrix > Citrix StoreFront / Web Interface > Server**
- the authentication settings under **Citrix > Citrix StoreFront / Web Interface > Logon**

➡ An FAQ document provides an overview of the features in the different versions.

## 6.3. Citrix ICA – global settings

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global**

This section describes the procedure for configuring the global Citrix settings. This configuration applies for all Citrix sessions.



These are the standard values for all Citrix sessions. Most of these properties, in particular the color depth, resolution and the server IP or server name, can be changed separately for each session.



Citrix Receiver 13 does currently not support Kerberos authentication.



Users can only change their expired password if this option has been enabled on the Citrix server. See FAQ Warning message when changing password.

### 6.3.1. Server location

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Server Location**

The **Server Location** option - also referred to as server browsing - allows you to bring up via the Citrix ICA client connected to the network a list of all Citrix servers and all published applications which are accessible via the network and use the selected browsing protocol.



The standard functionality for this option is **Auto-Locate** (Broadcast). With this function, the ICA client sends a "Get nearest Citrix server" package. The address of the first Citrix server to reply then functions as the master ICA browser.

You can also specify a separate **address list** for each network protocol. This can be

- TCP/IP
- TCP/IP + HTTP
- SSL/TLS + HTTPS

#### TCP/IP

If your network configuration uses routers or gateways, or if additional network traffic owing to transmissions is to be avoided, you can specify special server addresses for the Citrix servers from which the list of available servers and/or published applications is to be requested.



You can add a number of addresses to the address list so that the clients can establish a connection and function even if one or more servers are not available.

#### TCP/IP + HTTP

You can also call up information from the available Citrix servers and published applications via a firewall. To do this, you use the protocol **TCP/IP + HTTP** as the server location.



The **TCP/IP + HTTP** server location does not support the auto-locate function.

#### SSL/TLS + HTTPS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption offer server authentication and data stream encryption. They also allow you to check the integrity of messages.



If you try to establish a non-SSL/TLS connection to an SSL/TLS server, you will not be connected. A **Connection Failed** message will be shown.

### 6.3.2. Local logon

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Local Logon**

Use Kerberos pass-through authentication in all ICA sessions	<p>This option enables single sign-on for all ICA sessions if Log on to the thin client with AD/Kerberos is configured.</p> <p>The server too must be configured for pass-through authentication. When launching ICA sessions, it is then no longer necessary to enter a user name and password again as the local logon data (domain logon) are transferred for session logon purposes.</p> <p>Use the local logon module if problems with load balancing occur. The user's logon information is transferred when connecting to the metaframe master browser.</p>
Use local logon window	If this option is enabled, you will need to enter the password again when logging on.
Restart mode	The logon module is automatically restarted after being closed.
Type	Here, you can pre-populate the user name and domain in the logon window and choose between the settings from the last logon and the session setup.
Pre-populate logon information	The logon window is pre-populated with the user name and domain.
Show domain	Shows the domain entry in the logon window.
Use client name as user name	This setting may help to resolve reconnection problems during load balancing.
Allow logging on with smartcard	Only specific smartcard types are supported. You will find a list of compatible types in the <b>Smartcard</b> sub-section of the setup.
Domains	Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the <b>Domains</b> drop-down area in the logon module.
smartcard	Allows local access to smartcards and tokens from various manufacturers.

### 6.3.3. Window

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Window**

The following settings are configured under **Window**:

Standard number of colors	Specifies the standard color depth - the default setting is a color depth of 256 colors.
Approximate colors	Given the differences between the color palettes used by the ICA client and the "thin client" desktop, the screen may flash annoyingly if you switch between windows on a pseudo-color screen. The ICA client's color adaptation scheme prevents this flashing as it uses the colors from the local desktop palette in order to display the ICA window session. If <b>Approximate Colors</b> is enabled, flashing when switching between windows is avoided.
Window size	Specifies the width and height of the window.
Embed systray icons in window manager taskbar	Inserts an application icon into the local taskbar
Font smoothing	Enables font smoothing - in the event of performance problems, font smoothing should be switched off as it requires additional computing power.
Multi Monitor	Stipulates whether the full-screen mode is to be extended to all monitors.

### 6.3.4. Keyboard / hotkey assignment

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In MS Windows for example, the key combination **Alt+F4** closes the current window. It also works in ICA sessions too. All key combinations with **Alt** which are not used by the X Window Manager function in the familiar way during an ICA session.

The key alternatives are restricted to **Ctrl+Shift+Key** by default. However, you can change the settings by clicking on the **Hotkey Modifier** drop-down field and/or hotkey symbol for the relevant key combination.

- Possible keys: **F1 – F12**, **Plus**, **Minus**, **Tab**
- Possible modifiers: **Shift**, **Ctrl**, **Alt**, **Alt+Ctrl**, **Alt+Shift**, **Ctrl+Shift**



If you would like to use the PC key combination **Ctrl Alt Delete** during an ICA session, use the key combination **Ctrl Alt Enter** or **Ctrl Alt Return key**.

### 6.3.5. Mapping

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in ICA sessions.

## Drive mapping

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the thin client (including CD-ROMs and disk drives) is made available to you during ICA sessions on Citrix servers. On this page, you can specify which folders or drives are mapped during the logon. This then applies for all ICA connection sessions.

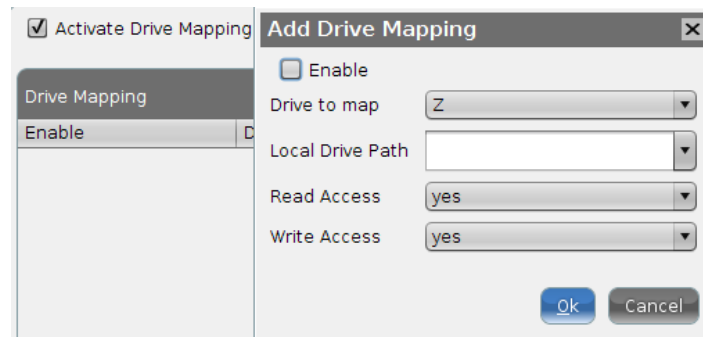


Figure 11: Drive mapping

The **Enable Drive Mapping** option allows you to temporarily enable/disable drive mapping. This offers the advantage that stored settings can be enabled or disabled without being lost.



Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices.

The procedure for setting up drive mappings is as follows:

1. Click on **Add** to bring up the mapping window.
2. Select a **target drive** from the list under which the local device or the folder is to be mapped.



If the drive letter you have selected is no longer available on the Citrix server, the specified directory or local drive will be given the next free letter during the logon.

3. Give the path name of the local directory to which the mapping is to refer.



If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated disk drive).

4. Specify the access authorizations for the mapping.

For each mapping, you have the option of granting **read access** or **write access**. You can also select the **Ask** option to query the read/write access rights when each ICA session is accessed for the first time.



The drive mappings and access data defined here are then valid for all ICA connections.

## COM ports - serial connections

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > COM Ports**

Enable **Com Port Mapping** in order to perform bidirectional mapping between serial devices connected to the thin client (e.g. scanners, serial printers) and the serial ports of the Citrix server.

As a result, programs running on the server can exchange data with the local devices.

- Click **Add** under **COM Port Device**.
- From the drop-down list, select the serial port to which a device is connected or click on **Detect Devices...** to select an available device.

Your selection will be mapped to the virtual COM1 connection. A second device will be mapped to the virtual COM2 connection and so on.

## Printers

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

With the **Enable Client Printer** function, the locally connected thin client printer is made available for your ICA sessions, provided that it was not disabled on the server side.

The printers must be set up on the **Devices→Printers→CUPS→Printers** page and must be enabled there for mapping in ICA sessions, see *ICA sessions* (page 35).

Because the thin client merely places incoming printer jobs in a queue, you need to install the printer on the server.

## Device support / virtual communication channels

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**

Enable virtual ICA channels for communicating with various devices connected to the thin client. These can be card readers, dictation machines or even USB storage devices. Channels of this type allow the device to communicate with the relevant server application.

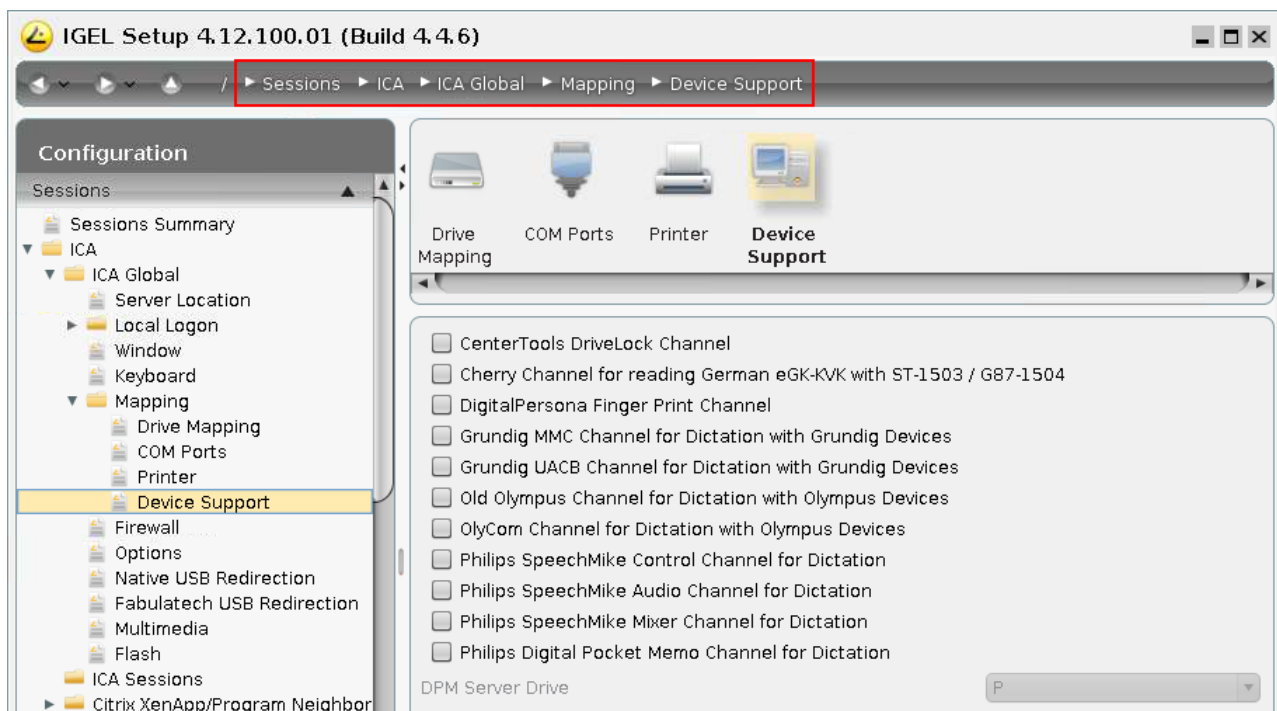


Figure 12: Supported devices



When using CenterTools DriveLock, ensure that the use of USB devices is not universally restricted: **Devices > USB Access Control**

## DriveLock

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**

The virtual DriveLock channel (ICA protocol) is included in the UDLX from Version 4.11.100 and must be installed on the Citrix-XenApp server.

DriveLock can read hardware data from local USB devices and transfer these data with the help of the Virtual ICA Channel Extension to the XenApp server. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

The following steps are important in order to be able to define the access rights for drives via the DriveLock server configuration:

- Enable the USB devices via drive mapping so that they are available as drives within your terminal session.
- Check the settings under **Sessions > ICA > ICA Global > Mapping > Drive Mapping**, they should correspond to the DriveLock settings.
- Disable Citrix USB redirection, because this will otherwise prevent drives being recognized by DriveLock.

- Check the device settings **Devices > Storage Devices > USB Storage Hotplug**, as they can influence the USB devices during the Citrix session.
- Install and enable the DriveLock channel in the Universal Desktop setup under **Sessions > ICA > ICA Global > Mapping > Device Support**.
- ➡ In the Centertools download area, you will find a document which describes in greater detail the procedure for configuring DriveLock on the server side: [How to use Centertools DriveLock with IGEL Thin Client \(PDF\)](#)

## DigitalPersona authentication

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**

By integrating DigitalPersona fingerprint readers into the thin client system and using the associated server software, users of IGEL thin clients can identify themselves through their fingerprints when using virtual applications on a Citrix XenApp server. All x86-based IGEL thin clients with the IGEL Linux operating system support the handling of logon data via the DigitalPersona Pro Enterprise Software (Version v5.3 and v5.4).

When used in conjunction with the DigitalPersona U.are.U 4500 fingerprint readers which are connected to IGEL thin clients via USB, the software provides a secure and quick means of authentication on virtual desktops.

In order to be able to use fingerprint readers in Citrix sessions, enable the relevant virtual channel in **Device Support**.

## Softpro SPVC Channel

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**

- Enable the **Softpro SPVC Signature Pad Channel** in order to use Softpro/Kofax pads in Citrix sessions.
- ➡ You will find detailed information regarding the configuration of signature pads in the Best Practice documents for StepOver Pads and Softpro/Kofax pads.



Figure 13: Softpro SPVC channel

## Nuance channel for dictation

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

- Enable the **Nuance Channel for Dictation** in order to use dictation solutions from the manufacturer Nuance in Citrix sessions.

### 6.3.6. Firewall

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Firewall**

<b>Use alternative address</b>	Define a proxy or secure gateway server as an alternative address for connections via a firewall. Note the tool tips regarding the individual configuration parameters.
<b>Secure Gateway (relay mode)</b>	If you would like to use a Citrix Secure Gateway in relay mode, you must give the full domain name – the IP address is not sufficient in this case.



After enabling the alternative address, add the server to the address list in the **Server Location** field in **Global Settings for ICA**.

### 6.3.7. ICA global options

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Options**

On this page, you can set up additional options to optimize the system's general behavior and its performance.



Use server redraw	The Citrix server is responsible for refreshing the screen content.
Disable Windows warning sounds	This option allows you to disable Windows warning sounds.
Use backing store	The X Server temporarily stores hidden desktop content.
Delayed screen update mode	Enables delayed updates from the local video buffer on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.
Caching	Allows you to change the settings for the bitmap cache. If you work with images that are displayed over and over again, you can significantly improve the performance of your ICA session(s). Specify the maximum amount of local system storage capacity (in kilobytes) used for temporary storage purposes. You can also specify the minimum size of bitmap files which are to be stored in the cache as well as the directory in which the files can be stored locally.



An excessively high setting can mean that the thin client has too little storage space for its own system and other applications. If in doubt, you can equip your thin client with additional RAM.

Scrolling control	Depending on the speed of your network or the response time of your server, there may be a delay between you letting go of the mouse button on a scroll bar and the scrolling actually stopping (e.g. when using EXCEL). Setting the value to 100 or higher may help to rectify this problem.
Enable auto-reconnect	Allows you to specify the parameters for reconnecting the session
Allow Kerberos pass-through in Program Neighborhood sessions	Allows the use of Kerberos pass-through authentication in the Citrix Program Neighborhood session.

### 6.3.8. USB redirection

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Native USB Redirection / Fabulatech USB Redirection**

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible.

Use either **Native USB Redirection** or **Fabulatech USB Redirection**.

For **Fabulatech USB Redirection**, a special Fabulatech server component must be installed on the Citrix server (USB for Remote Desktop Igel Edition).

➔ More detailed information on the function can be found on the Fabulatech partner site:  
<http://www.usb-over-network.com/partners/igel/>.



Enable either native or Fabulatech USB redirection – not both together.  
Disable USB redirection if you use Centertools DriveLock (page 30).

### 6.3.9. Multimedia redirection

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > HDX Multimedia**

Citrix HDX multimedia acceleration improves playback via Media Player within an ICA session on the remote desktop and allows isosynchronous transmissions, e.g. of webcams within the session.

See *Supported formats and codecs* (page 9).

☒ Enable Multimedia Redirection

☒ HDX Realtime WebCam Redirection

HDX WebCam frame rate: 5

HDX WebCam quality: 16

HDX WebCam width: 352

HDX WebCam height: 288

HDX WebCam delay time: 2000

HDX WebCam delay type: 1

☐ Enable HDX Realtime Media Engine

☐ Enable Content Redirection

Figure 14: Multimedia redirection

To improve multimedia playback on the remote desktop, follow the procedure below:

1. To take advantage of improved playback, ensure that the necessary codecs are installed on the remote desktop page.
2. Enable multimedia redirection on the thin client.
3. Create the session.
4. Begin playback on the remote desktop.

### 6.3.10. Flash redirection

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > HDX Flash**

Depending on the performance of the thin client, Citrix HDX Mediatream Redirection for Flash allows smoother playback of Flash content than is possible within the Citrix session itself.



An installed Flash Player browser plug-in is needed in order to enable flash redirection. Install the plug-in under **Sessions > Browser > Plug-Ins > Fash Player**.

### 6.3.11. Codec

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Codec**

For the Citrix 13.x Versions, two codecs for reproducing display content are available to choose from:

- The standard setting **Automatic** automatically selects the appropriate codec according to the performance of the hardware.
- Alternatively, the codecs **H.264** (for high-quality complex graphics) and **JPEG** (less CPU-intensive) as well as their options can also be selected manually.



If Version 12.x of the Citrix Receiver is selected, this setup page cannot be edited.

## 6.4. Citrix ICA – Sessions

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions**

If a session is created or edited, you can change the ICA session settings if they differ from the global settings.



The primary source of further information relating to Citrix connections should always be the relevant Citrix documentation. This manual merely gives general configuration tips.

### 6.4.1. Server

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Server**

Browser protocol	Allows you to select the protocol needed for transmission or the global standard setting
Do not use standard server location	Lifts the standard server requirement – for each protocol separately
Server	<p>By clicking on the <b>Search</b> button, you send a transmission signal which queries all available servers and published applications.</p> <ul style="list-style-type: none"> <li>By selecting the server, the user is connected to the entire desktop as if logging on at the server itself. As a result, all applications, rights and settings contained in the user's profile (local server profile) are available.</li> <li>If one of the published applications is selected, the session is opened in a window which contains just one application. The session is ended if you close this application.</li> <li>You can also manually enter the IP address or the host name of the server in the <b>Server</b> field.</li> </ul>
Application	If you have entered the server manually, you can specify a published application here. These fields are automatically filled in if you have selected one of the recognized published applications.
Working directory	Details of the path name of the work directory for the application

### 6.4.2. Logon

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Logon**

Use Kerberos pass-through authentication	Enables single sign-on for this ICA session if Log on to the thin client with AD/Kerberos is configured. The server too must be configured for pass-through authentication. When launching the ICA session, it is no longer necessary to enter a user name and password again.
Use pass-through authentication	Enables single sign-on for this ICA session if Log on to the thin client with AD/Kerberos is configured. The fact that the user name and password are temporarily stored when logging on to the thin client means that they no longer need to be entered again when launching a session.
User, password, domain	A user name, password and domain for the ICA session can be entered here. These details are automatically forwarded to the server and no longer need to be entered on the logon screen.
Hide password protection before logging on	This option switches the Windows splash screen on and off. This option must be disabled when logging on to Windows using a smartcard!

### 6.4.3. Window settings

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Window**

The following settings are configured under **Window settings**:

Number of colors	The color depth is set as a <b>global default</b> . You can change it for this session.
Use standard setting for color table	The color table is preset on a global basis. You can approximate it for this session.
Window size	By disabling the <b>full-screen mode</b> , you can choose between the global default setting and a session-specific setting.
Start monitor (Dualview)	Specifies which monitor in an environment with several monitors is to be used for the session.
Enable seamless window mode	The seamless window mode can only be used with published applications or with a specified start program for the server connection.
Font smoothing	Font smoothing is preset on a global basis. You can change it for this session.

### 6.4.4. Firewall

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA session > [session name] > Firewall**

In this area, you can configure the following firewall settings:

- **Use Alternative Address:** Define a proxy or secure gateway server as an alternative address for connections via a firewall. Note the tool tips regarding the individual configuration parameters.
- **SOCKS/Secure Proxy:** Select the standard proxy settings here or define the settings yourself.
- **Proxy Type:** If you use Secure (HTTPS), SSL/TLS or 128-bit encryption must be enabled in order for a secure connection to be established.
- **Secure Gateway (relay mode):** If you would like to use a Citrix Secure Gateway in relay mode, you must give the full domain name – the IP address is not sufficient in this case.



After enabling the alternative address, add the server to the address list under **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Server**.

### 6.4.5. Reconnect

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Reconnect**

You can edit **Global Settings for ICA** for the **Reconnect** option.

## 6.4.6. Options

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Options**

Under **Options**, you can optimize performance and system behavior within the ICA session.

<b>Compression</b>	Reduces the amount of data transmitted via the ICA session. This results in a reduction in network traffic to the detriment of CPU performance. If you connect your server(s) via WAN, you should use compression. If you use a relatively low-performance server and only work in one LAN, you should disable this option.
<b>Caching image data</b>	Enables caching in the cache memory (configured in the global ICA settings) for each session. This makes sense if you use a number of ICA sessions but only one or two sessions are critical from a network bandwidth point of view or are intensively used during the day. In this case, you should reserve the cache memory for these settings.
<b>Encryption method</b>	Encryption increases the security of your ICA connection. Basic encryption is enabled by default. You should therefore ensure that the Citrix server supports RC5 encryption before you select a higher degree of encryption.
<b>Audio transfer</b>	Transfers system sounds and audio outputs from applications to the thin client. These are then output via the speakers connected. The higher the level of audio quality you select, the more bandwidth is needed for transferring audio data.
<b>HDX latency reduction</b>	Improves the performance of connections with a high level of latency by immediately reacting to keyboard entries or mouse clicks. This makes the thin client feel more like a normal PC.
<b>Mouse click feedback</b>	The mouse pointer immediately turns into an hourglass symbol, thus providing visual feedback in response to a mouse click.
<b>Local text echo</b>	Displays text entered more quickly and avoids latency within the network. Select a mode from the drop-down list: <ul style="list-style-type: none"> <li>• Select <b>On</b> for slower connections (connection via WAN) in order to reduce the delay between the user entering text and the text being displayed on the screen.</li> <li>• For faster connections (connection via LAN), select <b>Off</b>.</li> <li>• Select <b>AUTO</b> if you are not sure how fast the connection is.</li> </ul>



HDX must be enabled and configured on the Citrix server for it to work.

### 6.4.7. Desktop integration

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch Options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.
- Enable **Restart** to restart this session after the connection is terminated.

## 6.5. Citrix StoreFront / Web Interface

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface**

Some of the settings are already configured under Global settings for ICA and in the *ICA session setup* (page 35).

- Select the start options for the Citrix XenApp session, see **Desktop integration**.

### 6.5.1. Server

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Server**

- Under **Server Location**, specify the master browsers in which published applications can be searched for.



You can set up up to 5 Citrix master browsers per domain. If the first browser is not available, the second will be queried and so on. Please note that multiple farms can be searched. You can therefore specify addresses for a number of server farms.

- Click on **Use Citrix XenApp Service Page** to obtain settings from the server and configure published applications via the Citrix XenApp service page.

### 6.5.2. Logging on and off

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Logon**

- Enable **Use Kerberos Pass-Through Authentication (Web Interface only)** in order to use local logon data for listing and launching applications. The option enables Single Sign-on for XenApp if logon with AD/Kerberos is configured on the thin client.
- Enable **Use Pass-Through Authentication** in order to use temporarily stored logon data for listing and launching applications.
- *Smartcard Authentication* (page 40) is available for StoreFront
- You can synchronize your Citrix password with that for **Screen Lock**.

## Smartcard

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Logon > Smartcard**

From IGEL Linux 5.06.100, it is possible to log on to Citrix StoreFront using a smartcard with Version 13.1.3 of Citrix Receiver. A **smartcard** type can be selected or a custom **PKCS#11 module** integrated here.

### 6.5.3. Options

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Options**

Specify audio, keyboard and display options if they differ from the global settings.

☒ Use server settings for all Options (Citrix XenApp)

☒ Client Audio  
☐ Overwrite local Client Audio setting with server setting

Audio Bandwidth Limit: medium

Color Depth: Global setting

Window Size: Seamless|Desktop

☐ Restrict full screen sessions to workarea

Handling of keyboard shortcuts: Server setting

Figure 15: Citrix Storefront Options

### 6.5.4. Appearance

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Apperance**

You can configure the XenApp/Program Neighborhood applications in such a way that they are displayed in various areas of the local system, e.g. on the local desktop or in the Start menu.

- Enable **Scale Symbols for the Start Menu** to automatically adjust the size of the application symbol.



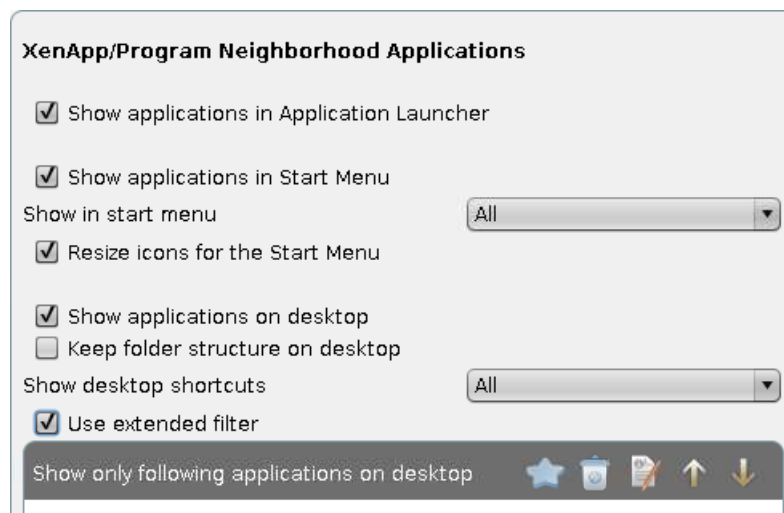


Figure 16: Citrix Storefront layout

### 6.5.5. Password Change

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Password Change**

Specify how a connection for changing a password is to be established.

Generic session	Searches for servers/applications and subsequently establishes a connection
Pre-configured ICA session	Selects a pre-defined ICA session according to session name
Citrix XenApp services site	Allows you to change a password via the Citrix Web Interface itself
Use Kerberos to change the password	If Kerberos authentication is set up on the XenApp Server, the password can also be changed via this route.

### 6.5.6. Reconnect and Refresh

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Reconnect / Refresh**

➤ Select the required option when reconnecting with sessions.

You can establish a connection

- during the logon process and
- through using a reconnect session, e.g. on the desktop.

With the help of the reconnect procedure, you can launch **active and terminated sessions, terminated sessions only** or **sessions on demand**.



A Refresh Session reloads the XenApp session without terminating it.

### 6.5.7. Log off

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Logoff**

If the **Use hotkey** option is enabled, you can log off from a session using a key combination. The combination consists of **modifier** keys such as **Ctrl** (Control), **Alt** and **Shift** and a number or a letter as a **hotkey**.

### 6.5.8. Desktop Integration

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.

## 6.6. Citrix Access Gateway

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix Access Gateway**

With the **Citrix Access Gateway (CAG)** client, you can establish a VPN connection to a CAG standard server 4.6. The VPN connection is an SSL tunnel. A certificate is transferred from the server to the client in the process. If the certificate is not trustworthy, a warning will be given when an attempt to establish a connection is made. In order to avoid the warning, the server certificate can be stored on the thin client in the `/wfs/cagvpn/cagvpn-trusted-CAs.crt` file. The warning can also be disabled in the CAG client configuration.

## 6.7. RDP – global settings

Menu path: **Setup > Sessions > RDP > RDP Global**

This section describes the procedure for configuring the global RDP settings. This configuration applies for all RDP sessions. The protocol version can no longer be configured manually, while the version used by the server is automatically recognized and used.

### 6.7.1. Remote Desktop Gateway

Menu path: **Setup > Sessions > RDP > RDP Global > Gateway**

Microsoft Remote Desktop Gateway allows remote access to Windows systems - with translation between the internal Remote Desktop Protocol RDP and the external HTTPS connection.

Access to the Remote Desktop environment takes place via browser which first establishes a secure connection to the gateway. The gateway forwards the connection request to the target system. At the same time, predefined Connection Access Policies and Resource Access Policies (CAP and RAP) for access control are evaluated.

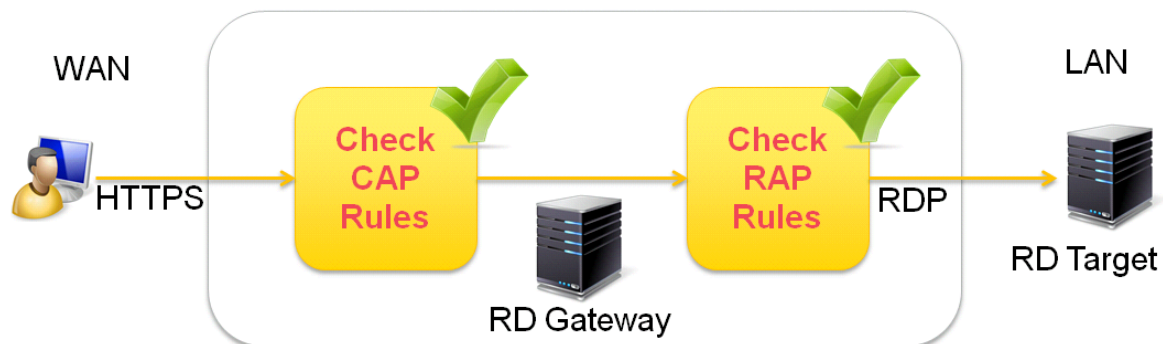


Figure 17: Remote Desktop Gateway

- Enable RD Gateway in **Sessions→RDP→RDP Global→Gateway** and enter the access data (no smartcard support).

RD Gateway requires Microsoft Windows Server 2008R2 or Server 2012 with various restrictions for each server version. The following Windows Server editions can preferably be used as gateway servers:

- Server 2008R2 Standard (limited to 250 RD Gateway connections)
- Server 2008R2 Enterprise
- Server 2008R2 Datacenter
- Server 2012 Standard
- Server 2012 Datacenter
- Server 2012 Essential (restricted to the RD Gateway role)
- Server 2012R2 Standard
- Server 2012R2 Essential (restricted to the RD Gateway role)

There is no support for RD Gateway in the IGEL RDP Legacy Mode (**RDP Global > Options**)!

### 6.7.2. Local Logon

Menu path: **Setup > Sessions > RDP > RDP Global > Local Logon**

**Local logon** allows user data pre-population, e.g. with data from the domain login, when establishing the connection to the terminal server. This can save you having to enter the same login data on a number of occasions.

You can also use **Local logon** to freely select the server in the login window of an RDP session.

Enable **Use local login window** to

- Pre-populate user data
- Freely select the server in the login window of an RDP session.

If the user data, e.g. the data from the domain login, are pre-populated, this can save you having to enter the same login data on a number of occasions.

Use local login window	If this option is enabled, you will need to enter the password in the RDP login window on the terminal side when logging in.
Pre-populate login information	The login window is pre-populated with the user name and domain.
Type	Here, you can pre-populate the user name and domain in the login window and choose between the settings from the last login and the session setup.
Show domain	Shows the domain entry in the login window.
Set client name as user name	This setting may help to resolve reconnection problems during load balancing.
Restart mode	The RDP login window is displayed in restart mode and cannot be closed.
Enable network authentication	Enables network authentication via NTLM. Smartcards are not supported here.
Domains	Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the <b>Domains</b> drop-down area in the login module.

### 6.7.3. Window

Menu path: **Setup > Sessions > RDP > RDP Global > Window**

In this area, you can configure the window for RDP sessions.

You can change the following settings:

- **Number of Colors:** Specifies the color depth.
- **Window Size:** Specifies the width and height of the window.
  - **Fullscreen:** The session is shown on the full screen. The thin client's taskbar is not visible.
  - **Workarea:** The session is shown on the full screen, minus the area needed by the thin client's taskbar.
  - **Numeric details:** The session is shown in the selected resolution or on the selected percentage of the screen area.
- **Enable Display Control:** If this option is enabled, the window size can be changed during the session.



If the window size is to be changed during the session, at least Windows 8.1 or Windows Server 2012 R2 must be running on the server.



It is not possible to change the window size during the session if the **window size** is set to **full screen** or **work area**.

- **Enable toolbar:** If this option is enabled, a symbol bar for minimizing and closing a full-screen session will be shown.



If the symbol bar is enabled, a session will be shown on one monitor only, even if **Multi Monitor Fullscreen mode** is set to **Expand fullscreen session onto all monitors**.

- **Enable internal Backing Store:** If this option is enabled, the window content will be saved in an internal buffer. In the event of an expose event, buffering ensures that the window content is obtained from the internal buffer rather than having to be retrieved from the server. This reduces the burden on the network.
- **Multi Monitor Fullscreen mode:** Stipulates whether the full-screen mode is to be extended to all monitors.

#### 6.7.4. Keyboard

Menu path: **Setup > Sessions > RDP > RDP Global > Keyboard**

Configure how the keyboard reacts within RDP sessions. The following options are available:

- **Cache** (enable or disable)
- **PC keyboard scan codes** (convert or send directly)
- **Keyboard hotkeys** (forward or execute locally)

➡ You can select the keyboard layout in the Session Configuration ("automatic" is the default).

#### 6.7.5. Mapping

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in RDP sessions.

### Drive Mapping

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available to the user. Specify which folders or drives are mapped during the login.

Via **Enable drive mapping**, you can temporarily enable/disable drive mapping. This offers the advantage that stored settings can be enabled or disabled without being lost.



Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices.

The procedure for setting up drive mappings is as follows:

1. Click on **Add** to bring up the mapping window.
2. Select a **target drive** from the list under which the local device or the folder is to be mapped.



If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

3. Give the path name of the local directory to which the mapping is to refer.



If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated disk drive).

## COM Ports

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > COM Ports**

As with locally connected mass storage devices, you can also map the thin client's local serial connections during an RDP session:

1. Click on **Enable Com Port Mapping**.
2. Add the required connection.



If your device has an additional multiport PCI card, more than 2 connections may be available.

## Printer

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Printer**

You can set up a printer for RDP sessions here.

With the **Enable Client Printer Mapping** function, the locally connected thin client printer is made available for your RDP sessions, provided that it was not disabled on the server side.

The printers must be set up on the **Devices > Printers > CUPS > Printers** page and must be enabled there for mapping in RDP sessions.

Because the thin client merely places incoming printer jobs in a queue, you need to install the printer on the server.

## Device Support / Virtual Communication Channels

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Device Support**

Enable virtual RDP channels for communicating with various devices connected to the thin client. These can be card readers (smartcards), dictation machines or even USB storage devices. Channels of this type allow the device to communicate with the relevant server application.

☒ Enable Plugin Support

☐ Cherry Channel 0 for reading German eGK-KvK with ST-1503 / G87-1504

☐ Cherry Channel 1 for reading German eGK-KvK with ST-1503 / G87-1504

☐ Grundig MMC Channel for Dictation with Grundig Devices

☐ Grundig UACB Channel for Dictation with Grundig Devices

☐ Olympus olyvc Channel for Dictation with Olympus Devices

☐ Philips SpeechMike Control Channel for Dictation

☐ Philips SpeechMike Audio Channel for Dictation

☐ Philips SpeechMike Mixer Channel for Dictation

☐ Philips Digital Pocket Memo Channel for Dictation

DPM Server Drive P:

---

☒ Enable Smart Card

## DriveLock

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Device Support**

The virtual DriveLock channel (RDP) is included in the UDLX from Version 5.01.100 and must be installed on the RDP server.

DriveLock can read hardware data from local USB devices and transfer these data to the server with the help of the Virtual RDP Channel Extension. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

The following steps are important in order to be able to define the access rights for drives via the DriveLock server configuration:

- Enable the USB devices via drive mapping so that they are available as drives within your terminal session.
- Check the settings under **Sessions > RDP > RDP Global > Mapping > Drive Mapping**, they should correspond to the DriveLock settings.
- Disable RDP-USB redirection, because this will otherwise prevent drives being recognized by DriveLock.
- Check the device settings under **Devices > Storage Devices > USB Storage Hotplug**, as they can influence the USB devices during the RDP session.
- Install and enable the DriveLock channel in the Universal Desktop setup under **Sessions > RDP > RDP Global > Mapping > Device Support**.
- ➡ In the Centertools download area, you will find a document which describes in greater detail the procedure for configuring DriveLock on the server side: [How to use Centertools DriveLock with IGEL Thin Clients \(PDF\)](#)

## Sound

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Sound**

Allows you to enable local audio playback.

### 6.7.6. Performance

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

In the event of performance-related problems, disable graphics functions which are not absolutely necessary. In low-bandwidth environments, you should use compression in order to reduce the network traffic.



This uses additional CPU power.

## RemoteFX Support

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

With the Service Pack 1 for Windows Server 2008 R2, local system functions such as Windows Aero or 3D display can be made available in RDP sessions too. In order to do this, the RemoteFX extension for RDP must be enabled. You can configure the relevant settings under **RDP Global → Performance** or on the corresponding session settings.

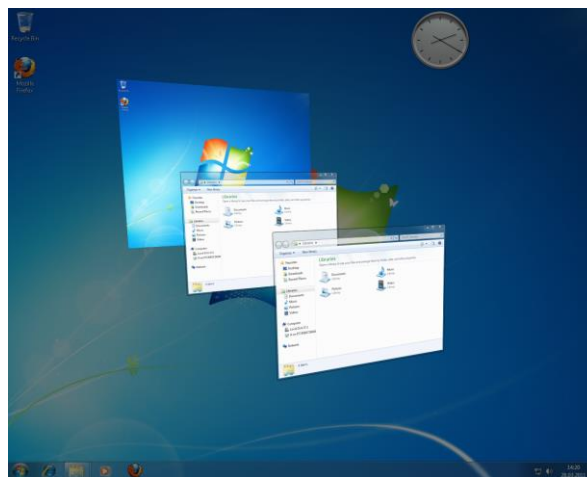


Figure 18: Windows Aero

Globally enabling Remote FX is not recommended as conventional RDP sessions may also be affected by this. With RemoteFX, all graphics effects available under Performance are enabled. This may slow down the session as a result. It is better to enable the function only for individual sessions which establish a connection to appropriately equipped servers.



➡ Further information on Remote FX and the server-related requirements is available from Microsoft at <http://technet.microsoft.com/en-us/library/dd736539%28WS.10%29.aspx>.

In the IGEL Registry, you can configure the number of frames sent by the server without confirmation under the key `rdp.winconnect.remotefx-ack`. The standard value is 1. A value of 2 or 3 can lead to improved performance in networks with high latency times.

### 6.7.7. Options

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

Disable Mouse Motion Events	Instructs the client not to show "unnecessary" cursor movements in order to conserve power.
Reset License	If you have to remove the MS license from the device, enable this option and restart the device.
Client Name	Give a client name for terminal service identification - the standard setting is the host name of the computer.
Enforce TLS encrypted connection	Permits TLS-encrypted connections only / verifies server certificates / deletes certificates that are no longer needed
RDP Legacy Mode	Switches to prior (IGEL Linux v4.x) RDP client version - see note below!



Before using **RDP Legacy Mode** to solve any occurring problem with the current RDP client (IGEL Linux v5) please contact IGEL support to address your issue. **RDP Legacy Mode** may be removed with any later version of IGEL Linux.

### 6.7.8. USB Redirection

Menu path: **Setup > Sessions > RDP > RDP Global > Native USB Redirection**

Menu path: **Setup > Sessions > RDP > RDP Global > Fabulatech USB Redirection**

USB devices can be permitted or prohibited during an RDP session on the basis of rules. Sub-rules for specific devices or device classes are also possible.

Use either **Native USB Redirection** or **Fabulatech USB Redirection**.

For **Fabulatech USB Redirection**, a special Fabulatech server component must be installed on the server (USB for Remote Desktop Igel Edition).

➡ More detailed information on the function can be found on the Fabulatech partner site: <http://www.usb-over-network.com/partners/igel/>.



- Enable either native or Fabulatech USB redirection – not both together.
- Disable USB redirection if you use Centertools DriveLock (page 30).

### 6.7.9. Multimedia

Menu path: **Setup > Sessions > RDP > RDP Global > Multimedia**

To improve video playback on the remote desktop, follow the procedure below:

1. To take advantage of improved playback, ensure that the necessary codecs are installed on the remote desktop page.
2. Enable **Video Redirection** on the thin client.
3. Create the session.
4. Begin playback on the remote desktop.

## 6.8. RDP session

Menu path: **Setup > Sessions > RDP > RDP Sessions**

The following configuration pages offer you detailed setup options for the session:

<b>Server and logon</b>	Allows you to specify a server and a start application for the terminal server session. The necessary logon information is configured here. Otherwise, the terminal server logon window for entering the user and the password will be displayed.
<b>Gateway</b>	Allows you to enable gateway support. Logon data for RD Gateway may also be specified here.
<b>Window</b>	Allows you to specify the size of the session window and the color mode. The local task bar can be configured so that it remains visible during a full-screen session.
<b>Keyboard</b>	Allows you to specify the keyboard layout, scan codes and the direct connection between keyboard input and the Windows Server.
<b>Mapping</b>	Allows you to specify the audio output device (local/remote) and determine how key strokes and clipboard content are handled. The mapping of serial connections and local drives can be enabled for a session.  You can make connected mass storage devices available to the user using the appropriate mapping: Select <b>Enable</b> , choose the drive letter and the device to be mapped.
<b>Performance</b>	Allows you to disable non-essential graphical functions such as skin styles, window animation etc. This is useful in the event of performance problems.
<b>Options</b>	Allows you to specify the start application and the work directory for use during the session (how authentication errors are handled during the logon procedure). If, when connecting to the server, a terminal server gateway is to be used, you can configure the relevant settings here (No Gateway is pre-set).
<b>USB redirection</b>	Allows you to specify native USB redirection
<b>Multimedia</b>	Allows you to specify video redirection.

### 6.8.1. Server

Menu path: **Setup > Sessions > RDP > RDP Sessions > [session name] > Server**

In this area, you can overwrite the following server connection details and thus the standard settings:

- Choose between **Server** and **Enable RemoteApps Mode**.

#### Server

To set up a server, proceed as follows:

1. Give the **Server** name or the IP address.
2. Define the **RDP Port** which is to be used for the connection.  
The default port is 3389.
3. Under **Application**, specify a start-up application for the terminal server session.
4. Specify the **Working Directory**.
5. Enable **Changeable Server-URL on Local Logon** in order to allow the server to be entered freely. You must have enabled local logon in order to do this.

Otherwise, the terminal server logon window will be displayed for you to enter a user name and password. If the local logon is used (see above), the thin client's logon window. will be shown.



If the **Pass-Through Authentication** option is enabled, the session with the local logon data for the terminal user, e.g. from the domain logon, is used. However, this setting will be overridden by the **Local Logon** global parameter. You should therefore not use both options at the same time.

#### Microsoft RemoteApp

- Like the published applications of a Citrix server, MS Windows Server 2008 offers the option of passing on RemoteApps to the thin client. Detailed instructions regarding server configuration can also be found on the Microsoft website: TS RemoteApp Step-by-Step Guide.

On the client side, only a few parameters need to be configured after enabling the RemoteApp mode.



Please note that the name of the application to be launched must be preceded by two pipe characters (| |), e.g. | |Excel.

### 6.8.2. Display, Keyboard and Mapping

Menu path: **Setup > Sessions > RDP > RDP Sessions > [session name] > Window / Keyboard / Mapping**

- Under **Window**, specify the color depth, window size and the multiscreen behavior.
- Under **Keyboard**, configure the keyboard layout and the hotkey properties.
- Enable/disable the **allocation** of resources for the client, e.g. COM port or printer mapping.

The *global parameters* (page 42) are the default setting.

### 6.8.3. Performance and options

Menu path: **Setup > Sessions > RDP > RDP Sessions > [session name] > Performance / Options**

Specify the performance settings for the session if they differ from the *global configuration* (page 42).

Enable RemoteFX	Global setting ▼
Disable Wallpaper	Global setting ▼
Don't show contents of window while dragging	Global setting ▼
Disable Menu and Window animation	Global setting ▼
Disable Themes	Global setting ▼
Disable Cursor Shadow	Global setting ▼
Disable Cursor Settings	Global setting ▼
Enable font smoothing	Global setting ▼
Compress	Global setting ▼

Figure 19: Performance settings

## 6.9. Remote desktop web access

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access**

With Web access for remote desktop (Web Access for RD), users can access RemoteApp and a remote desktop connection via the start menu on a computer or via a web browser. RemoteApps and remote desktop connections therefore provide a modified view of RemoteApp programs and virtual desktops for users.

➡ More information on Web access for remote desktop can be found under Microsoft Technet - Web Access for RD

### 6.9.1. Configuring Remote Desktop Access

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access> Server**

There are three different modes for user access to RemoteApps. Two can be configured here:

- *Predefined configuration* (page 53) - Define several server connections with the same user credentials. The user has to enter their credentials and domain into the login mask.
- *Ask user* (page 54) - The connection has been configured on the server. The user just has to enter their corporate email address.

Or choose the third mode:

- *Via Browser* (page 55) - Access via browser

#### Predefined configuration

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access> Server**

Setting **Predefined configuration**:

1. Click **Remote Desktop Web Access->Server**.
2. Select **Predefined configuration** in the selection field **Server configuration**.
3. Create a new **Server location**.

- ➔ Find more information concerning session settings under *Connections* (page 56).

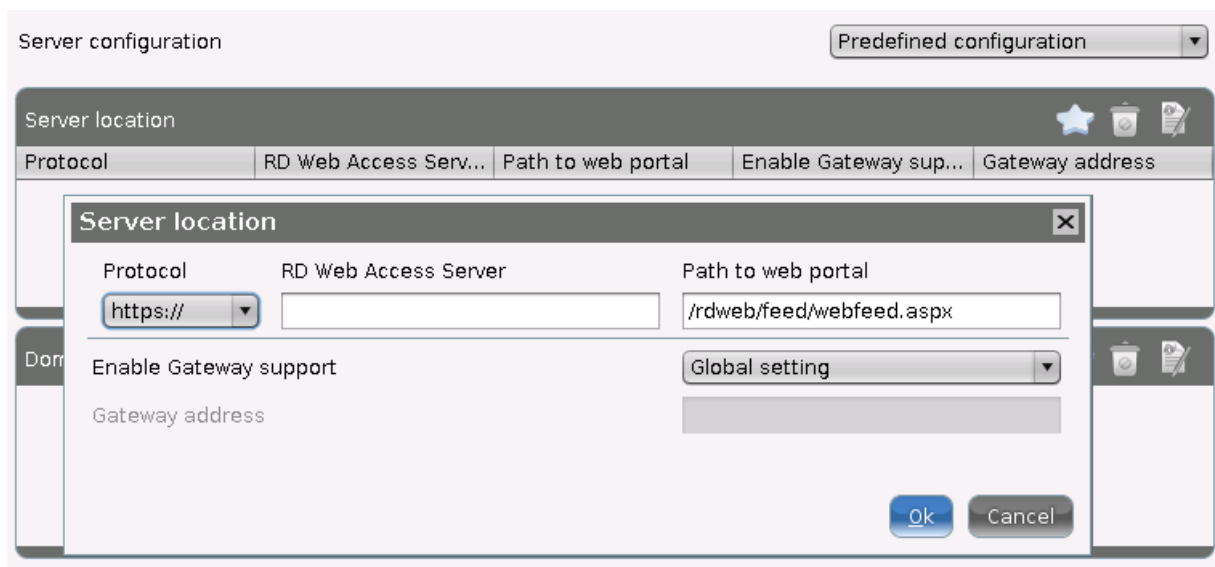


Figure 20: New RD Web Access Session

- If you have chosen **Predefined configuration**, there are two login modes available for user authentication: normal **User logon** or **Kerberos-Passthrough**. Set this configuration under *Authentication* (page 57).
- Define the logon/logoff mode under **Logoff / Desktop Integration** (page 58).



For the logon icon you have to make a setting, because it is not predefined. Otherwise you will not have access to the Web Access logon.

Provide the applications in the **Application Launcher**, in the **Start menu**, in the **Quick Start Panel** or even on the **Desktop**. Under **Appearance** you can select from a list of available applications to display them on the desktop or in the quick start panel.

## Ask User

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

This is a very user-friendly Web Access login.

In order to use it, the network connections connected with the user name on the server side must be pre-configured and it must be possible to query them via DNS.

To configure the **Ask user** login, proceed as follows:

- Select **Ask user** under **Server configuration**.

When logging in via RD Web Access, the user will be given a login window where they must only enter their corporate e-mail address, i.e. <name>@<domain>:



Figure 21: Ask User

## Via Browser

The Web Access page for Windows Server 2012 and Windows Server 2012 R2 can also be used on a Linux thin client in the Firefox browser.

- The user only needs the corresponding URL which is entered in the address bar.
- They then log on on the browser page using their user name and password.

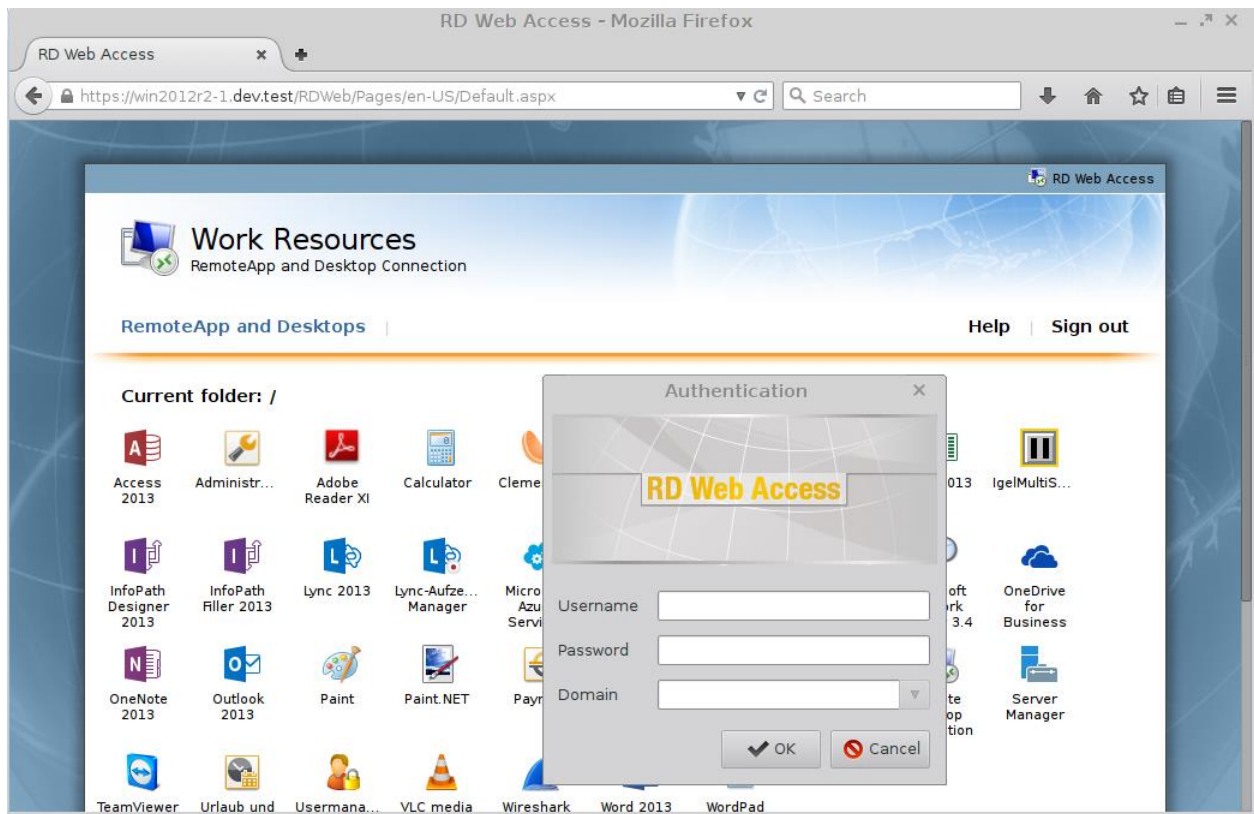


Figure 22: Remotedesktop Web Access in Firefox

If the user clicks on one of the applications offered by Web Access, the thin client will open a logon mask and then a remote desktop session for the chosen application.

### 6.9.2. Connections

Menupath: **Setup > Sessions > RDP > Remote Desktop Web Access > Connections**

In this area, you can define the connections to server locations and domains:



Figure 23: Remotedesktop Web Access



For the **pre-defined configuration**, specify the following values:

1. Select the **protocol** http:// oder https://.
2. Enter the name of the **Remote Desktop Web Access Server** and the path to the **web portal**.
3. If you would like to **Enable gateway support**, you can choose between the settings that you have made globally or in a custom session

If you would like to carry over the **session settings**, you must also specify the **gateway address**.

### 6.9.3. Authentication

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access> Appearance**

In this area, you can specify how you would like to log on to the RD Web Access session if you have opted for **Pre-defined configuration** under *Server* (page 56).

Figure 24: Web Access Authentication

Opt for one of the following authentication methods:

<b>User logon</b>	A logon window with the standard entry mask appears. The user enters their personal access data.
<b>Passthrough authentication</b>	The AD user data are passed on via Kerberos.
<b>Auto logon</b>	If you select this mode, the <b>User name</b> , <b>Password</b> and <b>Domain</b> fields are enabled to allow entries. The logon data are thus pre-set.

### 6.9.4. Appearance

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Appearance**

In this area, you can decide where you would like to display **RD Web Access applications**:

- In the **start menu**
  - In the **Application Launcher**
  - On the **desktop**
- Enable **Apply display filter** in order to restrict the applications shown to a specific selection.
  - Under **Add**, enter the name of the application that you would like to display on the desktop.
  - You can also select applications that you would like to display in the **Quick Start Panel**.

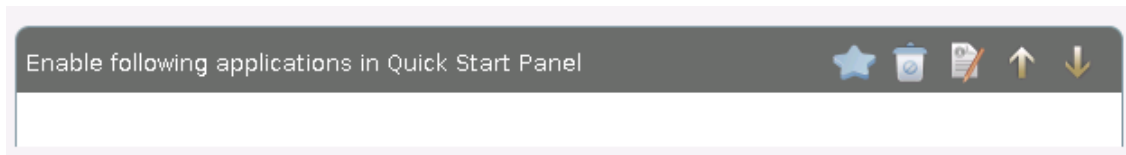


Figure 25: Configuring Quick Start Panel

### 6.9.5. Logoff / Desktop Integration

Menu path: **Setup > RDP > Remote Desktop Web Access > Logoff**

In these two areas, you can specify how you would like to log on to or log off from the application:

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch Options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.

Enable **Restart** to restart this session after the connection is terminated.

## 6.10. Horizon Client Global

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global**

In this area, you can define the global settings for Horizon Client sessions.

The following settings are carried over from the global settings for RDP sessions; see *RDP Global* (page 42):

- **Drive Mapping**; see *Drive mapping (RDP)* (page 45)
- **Number of Colors**; see *Window - RDP* (page 44)
- **Window Size**; see *Window - RDP* (page 44)
- **Multi Monitor Fullscreen Mode**; see *Window - RDP* (page 44)

## 6.10.1. Server options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Server Options**

In this area, you can specify the settings for the connection between the Horizon Client and the server.

- **Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.



If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- **Server setting:** The client does not give the server details of a preferred connection protocol. The connection protocol preferred by the server is used.
- **RDP:** The client tells the server that it prefers RDP as the connection protocol.
- **PCoIP:** The client tells the server that it prefers PCoIP as the connection protocol.
- **Enable kiosk mode:** If this option is enabled, Horizon Client sessions will be held in kiosk mode.
- **Server certificate verification mode:** Specifies what will happen if server certificate verification fails.

Possible values:

- **Reject if verification fails**
- **Warn if verification fails**
- **Allow unverifiable connections**

## 6.10.2. Local logon

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon**




In this area, you can pre-configure user data. As a result, you can avoid users possibly having to log on a number of times.

You can change the following settings:

- **Use local login window:** If this option is enabled, the local logon window of the thin client will be used to log on to the server. If you use the local logon window, you can pre-configure logon information.
- **Preset login information:** If this option is enabled, logon information will appear automatically in the logon window. With **Type**, you can specify the source of the logon information.
- **Type:**
  - **set user/domain from last login:** If this option is enabled, the logon information from the last session will appear automatically in the logon window.
  - **set user/domain from session setup:** If this option is enabled, session-specific logon information will appear automatically in the logon window. The session-specific logon information is described under *Connection Settings* (page 62).
  - **set user/domain from appliance mode:** If this option is enabled, the logon information specified in the appliance mode for VMware Horizon will appear automatically in the logon window; see *Appliance Mode* (page 66).

- **Show domain:** If this option is enabled, the domain will be shown in the logon window.
- **Relaunch mode:** If this option is enabled, the logon window will be shown in restart mode and cannot be closed.
- **Exit on disconnect or when an error occurs:** If this option is enabled, the session will be ended completely when the connection is terminated. If this option is disabled, the connection overview will be shown when the connection is terminated.

Working with domains:

- To create a domain, click on .
  - To remove a domain, click on .
  - To change a domain, click on .
- ➡ Further settings options can be found under *AD/Kerberos Configuration* (page 174) and *AD/Kerberos* (page 173).

### 6.10.3. USB redirection

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > USB Redirection**


In this area, you can enable and configure USB redirection for specific devices.

You can change the following settings:

To enable **USB redirection**, proceed as follows:

1. Enable the option **Enable USB Redirection**.
2. Select a **Default Rule**. The set rule specifies whether USB redirection is allowed or prohibited.
3. Create one or more rules for classes of devices or individual devices.

To create a **class rule**, proceed as follows:

1. To create a new rule, click on  in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Family**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Storage Devices**.
4. Under **Name**, give a name for the rule.
5. Click on **Ok**.
6. Click on **Apply** or **OK**.


The rule is active.

To create a **device rule**, proceed as follows:



When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** must be given.



1. To create a new rule, click on  in the **Device Rules** area.
2. Choose a **Rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.
5. Under **Name**, give a name for the rule.
6. Click on **Ok**.
7. Click on **Apply** or **OK**.

The rule is active.

#### 6.10.4. Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Multimedia**

You can change the following multimedia settings:

- **Enable VMware Multimedia Redirection**

Possible values:

- **off**: The server renders the multimedia data and sends the individual images to the client.
- **on**: The client renders the multimedia data supplied by the server.

- **Real Time Audio Video (RTAV)**: Specifies the redirection of video data from the client USB webcam.

Possible values:

- **off**: The client does not forward the webcam data as video data.



With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled.

- **on**: The client forwards the webcam data as video data.

#### 6.10.5. Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Performance**

In this area, you can optimize the performance of Horizon Client sessions.

You can change the following settings:

- **PCoIP client-side image cache size**: Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred.



Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

### 6.10.6. Smartcard

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Smartcard**

In this area, you can specify which smartcards are authorized when logging on.

## 6.11. Horizon Client sessions

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions**

### 6.11.1. Connection settings

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings**

In this area, you can specify the settings for the connection between the Horizon Client and the server.

- **Server URL:** URL of the VMware Horizon server
- **Use Passthrough authentication for this session:** If this option is enabled, the user name and password will be temporarily saved and used for authentication during this session.
- **Username:** User name when logging on to the VMware Horizon server
- **User password:** Password when logging on to the VMware Horizon server
- **Domain:** Domain when logging on to the VMware Horizon server
- **Session type:** Specifies whether the session contains a desktop or an individual application.

Possible values:

- **Desktop:** The session contains a desktop.
  - **Application:** The session contains an individual application.
  - **Desktopname:** Specifies a name for the desktop. This option is available if **Session Type** is set to **Desktop**.
  - **Application:** Application that is launched during the session. This option is available if **Session Type** is set to **Application**.
  - **Autoconnect:** If this option is enabled, the connection to the desktop or application will be established automatically when the session starts. For this to be possible, the name of the desktop or application must be defined. If this option is disabled, the overview will be shown when the session starts.
  - **Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.
  - **Enable kiosk mode:** If this option is enabled, the session will be held in kiosk mode.
- ➡ Further settings options can be found under *AD/Kerberos Configuration* (page 174) and *AD/Kerberos* (page 173).

### 6.11.2. Window

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Window**

In this area, you can change the way in which the session is displayed.

- **Window Size:** Specifies the width and height of the window.



The window size is carried over from the global settings for RDP sessions, see *Window* (page 44).

- **Number of Colors:** Specifies the color depth.



The color depth is carried over from the global settings for RDP sessions, see *Window* (page 44).

- **Start Monitor:** Specifies the monitor on which the session is shown.

➡ Further settings options can be found under *Screen* (page 116) and *Window* (page 44).

### 6.11.3. Mouse and keyboard

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mouse and Keyboard**

In this area, you can define the settings for the mouse and keyboard.

- **Disable mouse movement events:** If this option is enabled, the mouse pointer will only be shown locally on the thin client. If the user moves the mouse over a session item, no reaction of the item will be shown.

➡ Further settings options can be found under *Language* (page 131) and *Keyboard and Additional Keyboard* (page 134).

### 6.11.4. Mapping

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mapping**

In this area, you can specify the data transmission between the thin client and the Horizon Client session.

- **Enable Client Audio:** If this option is enabled, audio data are transmitted.
- **Enable Clipboard:** If this option is enabled, the clipboard will be available.
- **Enable Printer Mapping:** If this option is enabled, the printer will be available.
- **Enable Com Port mapping:** If this option is enabled, the COM port will be available.
- **Enable Drive Mapping:** If this option is enabled, the external drives will be available.
- **Enable USB Redirection:** If this option is enabled, the client's USB data will be forwarded to the server.

➡ Further settings options can be found under *Drive Mapping* (page 45), *Serial Connections (RDP)* (page 46), *Printers (RDP)* (page 46), *Audio* (page 48), *Keyboard* (page 45) and *Printers (Devices)* (page 161).

### 6.11.5. Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Performance**

In this area, you can save system resources by disabling certain visual functions of the user interface.

- **Disable Wallpaper:** If this option is enabled, no desktop background image will be displayed.
- **Don't show contents of window while dragging:** If this option is enabled, the content of a window will not be shown when the window is moved.
- **Disable Menu and Window animation:** If this option is enabled, transitions for menus and windows will not be animated.
- **Disable Themes:** If this option is enabled, desktop themes are not used.
- **Disable Cursor Shadow:** If this option is enabled, the mouse pointer will be shown without a shadow.
- **Disable Cursor Settings**
- **Enable font smoothing:** If this option is enabled, the edges of fonts will be smoothed.

➡ Further settings options can be found under *Performance (Horizon Global)* (page 61) and *Performance (RDP Global)* (page 48).

### 6.11.6. Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**

In this area, you can change various settings.

- **Working Directory:** Directory that will be used after login.
- **Compress:** If this option is enabled, the flow of data between the client and server will be compressed.
- **Force TLS encrypted connections:** If this option is enabled, the flow of data between the client and server will be encrypted with TLS.
- **Network Level Authentication:** If this option is enabled, the user will authenticate themselves on a network level (network layer authentication) in order to establish an RDP connection.



If network level authentication is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

➡ Further settings options can be found under *Options (RDP Global)* (page 49), *Performance (RDP Global)* (page 48) and *Local Logon (Horizon Global)* (page 59).

### 6.11.7. Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Multimedia**

You can change the following multimedia setting:

- **VMware multimedia redirection**

Possible values:

- **Global setting:** The global setting for Horizon Client sessions is used, see *Horizon Client Global Multimedia* (page 61).
- **off:** The server renders the multimedia data and sends the individual images to the client.

➡ Further settings options can be found under *Horizon Client Global Multimedia* (page 61).



### 6.11.8. Proxy

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Proxy**

In this area, you can configure the use of a proxy for the connection between the client and server.

You can change the following settings:

- **Direct Connection to the Internet:** If this option is enabled, no proxy is used.
- **Manual proxy configuration:** If this option is enabled, a proxy is used. The configuration must be specified in the following fields.
  - **HTTP Proxy:** URL of the proxy for HTTP
  - **Port:** Port of the proxy for HTTP
  - **SSL Proxy:** URL of the proxy for SSL
  - **Port:** Port of the proxy for SSL
  - **SOCKS Host:** URL of the proxy for SOCKS
  - **Port:** Port of the proxy for SOCKS
  - **SOCKS Protocol version:** Version of the SOCKS protocol used
  - **No Proxy for:** List of URLs for which no proxy is to be used.
- **Systemwide proxy configuration:** If this option is enabled, the proxy configured under **Setup > Network > Proxy** will be used.

➡ Further settings options can be found under *System-wide Proxy (Network)* (page 160).

## 6.12. Quest vWorkspace Client and AppPortal

Menu path: **Setup > Sessions > vWorkspace Client**

By default, **vWorkspace Client** session settings are carried over from the **RDP Global** setup pages. You can change the configuration for **vWorkspace Client** sessions (USB and multimedia redirection) on the relevant setup pages.

The **vWorkspace Client** is based on hypervisors from other providers and is therefore compatible with VMware, vSphere, Microsoft Hyper-V and XenServer.

➡ All configuration parameters for the **vWorkspace Client** and the **vWorkspace AppPortal Farm** are described in detail in the original documentation for the relevant client version, for Quest, see <https://support.quest.com/Default.aspx>.

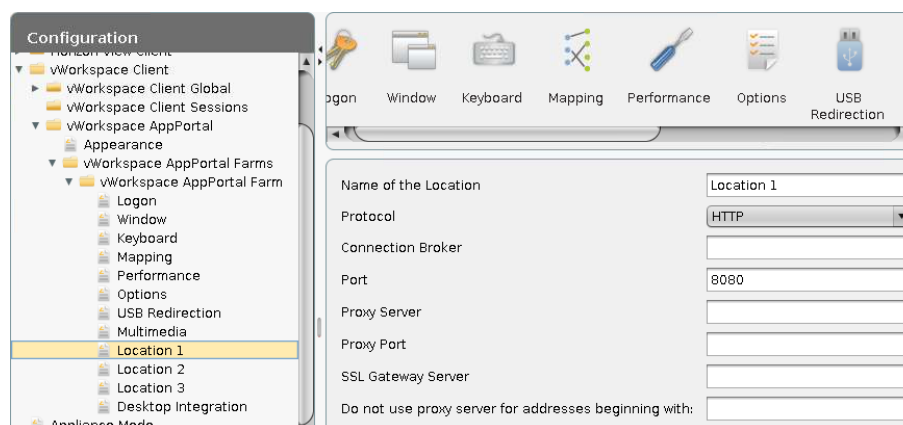


Figure 26: AppPortal farms configuration

## 6.13. Appliance mode

Menu path: **Setup > Sessions > Appliance Mode**

In the appliance mode, only a specific session is shown. Access to other applications is not possible.

To enable the appliance mode for a session type, proceed as follows.

1. Click on **Sessions > Appliance Mode**.
2. In the appliance mode pull-down menu, select the session type for which the appliance mode is to be enabled.

You can enable the appliance mode for one of the following session types:

- VMware Horizon
- Citrix XenDesktop (for published desktops only, not for published applications)
- RHEV/Spice
- Imprivata
- RDP Multipoint Server

3. Enter the necessary configuration data for the selected session type.



The system hotkey **Ctrl+Alt+S** for launching the setup application does not work in the appliance mode. Use **Ctrl+Alt+F2** instead.



You can set up a hotkey in order to launch quick setup in the appliance mode. You will find instructions for setting up the hotkey under *Desktop Integration* (page 23).

## Configuration data for VMware Horizon

- **Server URL:** URL of the VMware Horizon server
- **Username:** User name when logging on to the VMware Horizon server
- **User password:** Password when logging on to the VMware Horizon server
- **Domain:** Domain when logging on to the VMware Horizon server
- **Desktopname:** Desktop that is to be launched automatically
- **Autoconnect:** If this option is enabled, the desktop given in **Desktopname** will be launched automatically.
- **Network Level Authentication:** If this option is enabled, the user will authenticate themselves on a network level (network layer authentication) in order to establish an RDP connection.



If network level authentication is enabled, the local login window is used. This also applies if the **Use local login window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Login** is disabled.

- **Enable on-screen keyboard:** If this option is enabled and a touchscreen is available, an on-screen keyboard will be shown.



If the on-screen keyboard is enabled, the local login window is used. This also applies if the **Use local login window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Login** is disabled.

- **x coordinate of on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y coordinate of on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

## Configuration data for Citrix XenDesktop

- **XenDesktop delivery server URL:** URL of the XenDesktop Delivery server
- **Enable Smartcard Login:** If this option is enabled, the user can log on with a smartcard.



When the option is enabled, the browser and Xen will be restarted.

- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **x coordinate of on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **y coordinate of on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

## Configuration data for RHEV/Spice

- **Connection Broker:** URL of the connection broker
- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **x coordinate of on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **y coordinate of on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

## Configuration data for Imprivata

- **Set the URL to the Server:** URL of the single sign on server
- **Path to the application:** Path to the application on the single sign on server
- **Clear the Imprivata Data Partition:** If this option is enabled, the Imprivata data partition will be deleted.
- **Enable Logging of the Bootstrap Component:** If this option is enabled, the bootstrap component will generate a log.
- **Bootstrap Component's Logging Verbosity:** Specifies the logging level for the bootstrap component log.
- **generic session**
- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **X coordinate of on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y coordinate of on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

## Configuration data for RDP Multipoint Server

- **Connect to the server once it has been found:** The thin client will find one or more RDP Multipoint Servers itself if these are in the same network as the thin client and obtain their IP address from the same DHCP server as the thin client.

## 6.14. Leostream Connection Broker

Menu path: **Setup > Sessions > Leostream**

Specify a server, user and domain for logging on to Leostream Connection Broker. By default, the rdesktop Client is used for the connection in UDLX. rdesktop must therefore be set as the Leostream API protocol with priority 1 on the server.

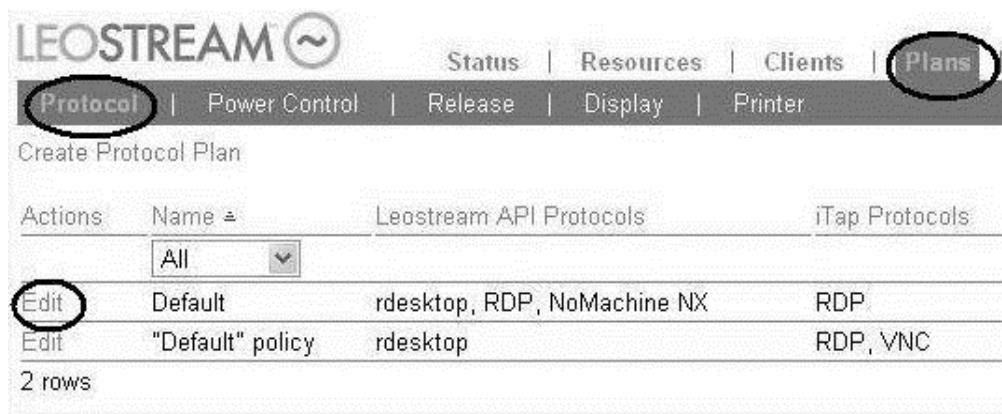


Figure 27: Leostream-API protocol

➡ More information on the Leostream Connection Broker is available from Leostream by visiting: <http://www.leostream.com/resources/downloads.php>.

## 6.15. Systancia AppliDis Client

Menu path: **Setup > Sessions > AppliDis**

AppliDis Fusion 4 is a virtualization solution which combines the virtualization of desktops and applications in a single console.

➡ The original documentation with a description of all parameters for the Systancia AppliDis Fusion 4 Client and the administration manual is available from Systancia Experts.

## 6.16. Evidian AuthMgr

Menu path: **Setup > Sessions > Evidian AuthMgr**

Using the **Evidian Authentication Manager (AuthMgr)**, you can log on to Citrix ICA, RDP and VMware Horizon roaming sessions using an RFID card. The Evidian AuthMgr can also execute user-defined commands.

➡ You can find setup instructions in a best practice document.

## 6.17. NoMachine NX

Menu path: **Setup > Sessions > NX**

If you configure an NX session, retain the NX server data and select the session type (Unix, Windows, VNC). Depending on the session type chosen, either the Unix Desktop, Windows Desktop or VNC Desktop setup pages are enabled to allow further configuration.

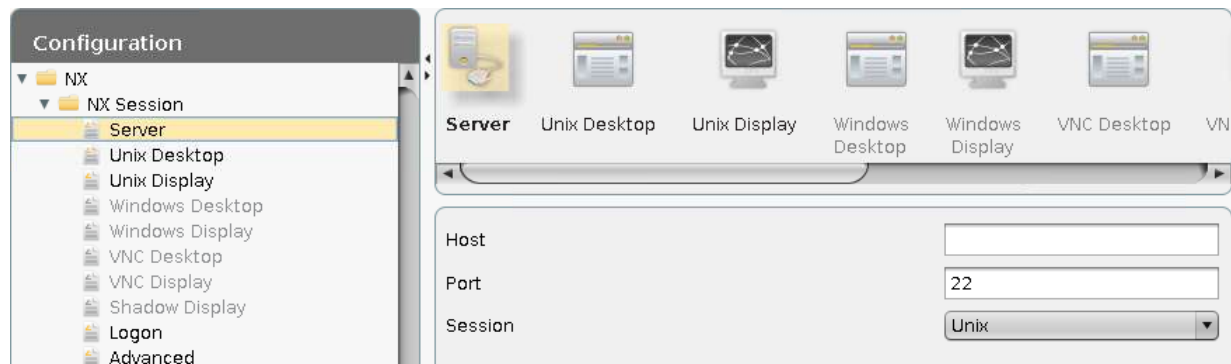


Figure 28: NX server configuration

The IGEL setup pages for NX sessions are essentially an adapted graphical user interface for the NoMachine NX Client.

➡ Further information regarding configuration (performance, services etc.) can be found in the original documentation provided by NoMachine: <http://www.nomachine.com/documents.php>.

## 6.18. X Session

Menu path: **Setup > Sessions > X Sessions**

Set up the basic connection data (type, server and command) on the server side and specify the necessary hotkey and window parameters in order to launch an X session.

## 6.19. Parallels 2X client session

Menu path: **Setup > Sessions > Parallels 2X Client**

Virtual desktops and applications can also be provided via 2X Application Server XG. A suitable client for access is included in IGEL Linux.

A more detailed description of all available parameters as well as information regarding use of the client is available from 2X:

- ➡ [http://www.2x.com/docs/en/manuals/html/clientlinux\\_manual/2XClientForLinux.html](http://www.2x.com/docs/en/manuals/html/clientlinux_manual/2XClientForLinux.html)
- ➡ <http://www.2x.com/docs/en/manuals/html/client-windows/2XClientForWindows.html>

## 6.20. PowerTerm WebConnect

Menu path: **Setup > Sessions > PowerTerm WebConnect**

With **PowerTerm WebConnect** you can access the following applications locally or remotely:

- Windows terminal server
  - remote desktops (VMware, Microsoft, Citrix and Virtual Iron)
  - Blade PCs
  - Legacy hosts
- Enter the host name of the WebConnect server you want to create a connection to.
- ➡ The server configuration is described in the Ericom documentation: PtSeriesUsersGuide\_LTC.pdf.

## 6.21. PowerTerm terminal emulation

Menu path: **Setup > Sessions > PowerTerm Terminal Emulation**

The PowerTerm InterConnect software we use in IGEL Linux is the official Linux version from ERICOM Software Ltd.



To use your Ericom PowerTerm Terminalemulation you need a free license key from IGEL. To get to the activation form please register at our support and ticket system.

To configure a session:

1. Click on **Add New Session**.
2. Select **PowerTerm** as the session type.

The **PowerTerm Emulation Setup** window opens.

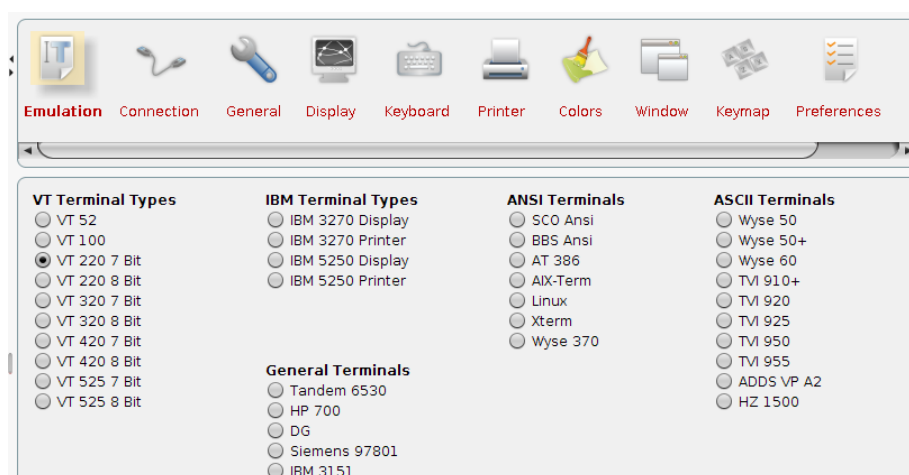


Figure 29: PowerTerm Emulation setup

This setup offers a good overview of the emulation types supported.

The setup pages used here were designed to look as similar as possible to the setup pages described in the original documentation from ERICOM Software Ltd.

➡ You will find detailed information on configuring the PowerTerm software in the PowerTerm manual on the Ericom documentation website.

### 6.21.1. PowerTerm selection

Two versions of the PowerTerm are available to choose from here:

- 10.1.0.0.20130211.2-\_rc\_-31580
- 9.2.0.6.20091224.1-\_rc\_-25848

Default, which corresponds to Version 9.2.0.6.20091224.1-\_rc\_-25848, is preset.

## 6.22. IBM iSeries Access

Menu path: **Setup > Sessions > IBM iSeriesAccess**

IBM iSeries Access for Linux (5722-XL1) offers emulation of the IBM-5250 terminal.

➡ A full description of the emulation is available from IBM by visiting:  
<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/index.jsp?topic=%2Frzatzv%2FrzatzvI5250.htm>.



The configuration is not accessible until the user confirms that the necessary license is available.



## 6.23. ThinLinc

Menu path: **Setup > Sessions > ThinLinc**

ThinLinc is a Linux terminal server solution which uses server based computing to virtualize desktops and applications. In addition to the ThinLinc framework itself, the package includes a VNC client for transferring the graphical information of the (virtual) remote desktop or application as well as OpenSSH for securing the connection by means of encryption.

In the session configuration, you can select display parameters such as the screen size, resolution or full-screen mode. You can also optimize the compression in order to conserve bandwidth. The SSH port can be adapted accordingly to meet your needs. The standard port 22 is pre-set.

You can map various local resources to a ThinLinc session:

- Printers
- Serial connections
- Local files, e.g. NFS with read and/or write authorization
- Audio devices such as audio output through local speakers

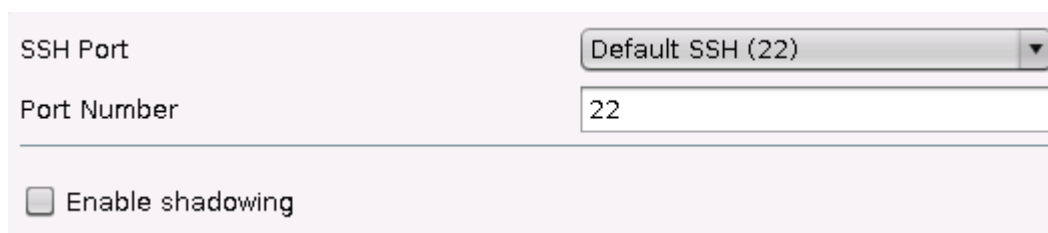
The desktop can be mirrored for the purposes of a ThinLinc session. This option is disabled by default.

➡ You will find further information on setting up the session in the "Client Configuration" chapter of the ThinLinc administration handbook: <http://www.cendio.com/resources/docs/adminguide.pdf>.

### 6.23.1. ThinLinc Global Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Server**

In this area, you can define settings for the ports.



SSH Port	Default SSH (22) ▼
Port Number	22
<input type="checkbox"/> Enable shadowing	

Figure 30: ThinLinc Port

- Select the **server port** for the SSH connection:
  - Standard SSH (22)
  - HTTP (80)
  - Other
- Specify the **port number** of the ThinLinc server.
- Decide whether you want to **Enable shadowing** in the session.

### 6.23.2. ThinLinc Global Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Window**

In this area, you can define the window settings for a **ThinLinc** session.

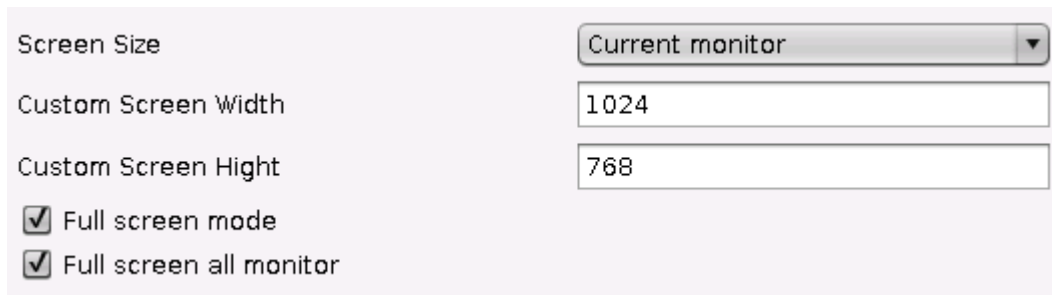
The screenshot shows the 'ThinLinc Global Window' settings interface. It features a light gray background with several configuration options. At the top, 'Screen Size' is set to 'Current monitor' via a dropdown menu. Below this, 'Custom Screen Width' is set to '1024' and 'Custom Screen Height' is set to '768' in text input fields. At the bottom, there are two checked checkboxes: 'Full screen mode' and 'Full screen all monitor'.

Figure 31: ThinLinc Window settings

- Select from the following **Screen Sizes** for the session:
  - 800x600
  - 1024x768
  - 1280x1024
  - 1600x1200
  - Current monitor
  - All monitors
  - Work area (maximized)
  - Custom size
- Define the **width** and the **height** of the session window.
- Enable **Full-screen mode** if you would like the session to fill the entire screen.
- Enable **Full screen all monitors** if the full-screen mode is to be extended to all monitors during multi-monitor operation and details of the arrangement of the monitors in the session are to be passed on so that maximizing windows in the session takes into account the size of the individual monitors for example.

### 6.23.3. ThinLinc Global Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Options**

In this area, you can specify further settings:

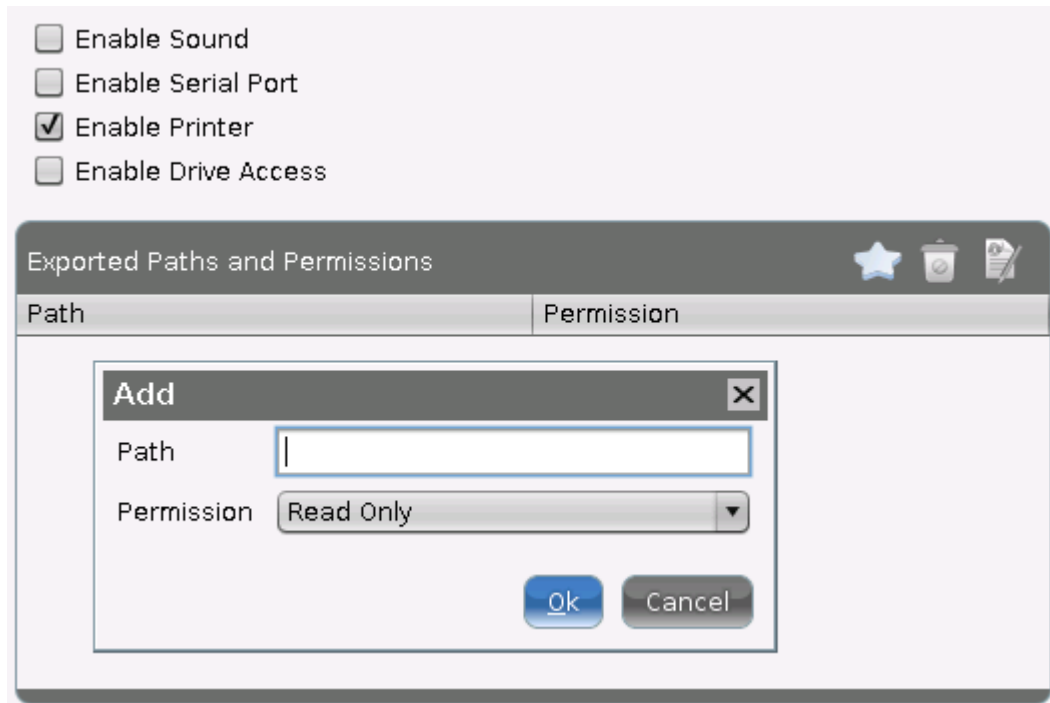


Figure 32: ThinLinc Optionen

- You can share local directories and specify access permissions for the server.

### 6.23.4. ThinLinc Global Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization**

In this area, you can increase the transmission speed by setting various compression procedures.

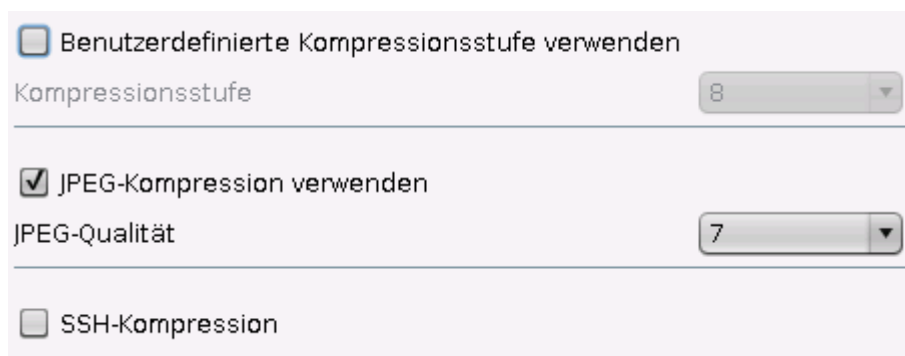


Figure 33: ThinLinc Optimierung

- Enable **Use user-defined compression level** in order to make your own settings. [9] is the highest level of compression.



A higher compression level saves bandwidth but requires more computing power.

- Enable **Use JPEG compression** in order to compress images. [9] is the highest level of compression.



A higher JPEG compression level saves bandwidth but reduces the image quality.

- Switch on **SSH compression** if you would like to use compression via Secure Shell.

### 6.23.5. ThinLinc Global VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization**

In this area, you can specify your **VNC Optimization options**:

Figure 34: VNC Optimization

- Enable **VNC autoselect** in order to set the encoding and color depth automatically.
- Disable **VNC autoselect** in order to make manual settings:
  - Specify the encoding for VNC:



Figure 35: VNC Encoder

- Specify the number of colors that are to be used:

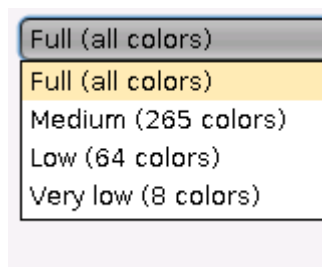


Figure 36: VNC Color Depth

### 6.23.6. ThinLinc session user interface

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session name]**

In a **ThinLinc** session, you can make the same settings as under **ThinLinc Global**.

You also have the option of changing the **user interface** of the ThinLinc login mask here:

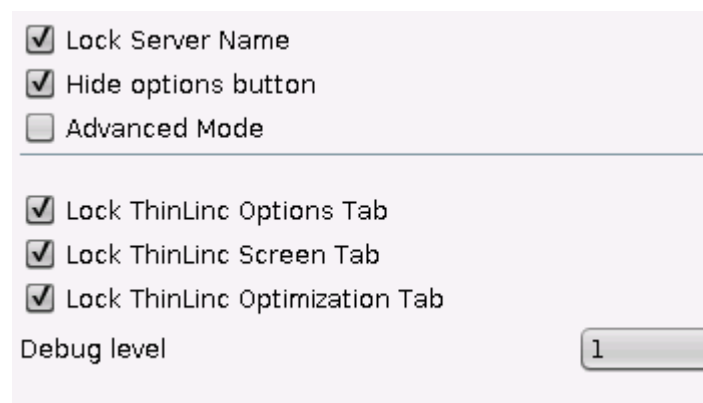


Figure 37: ThinLinc Session

- Lock various editing options.
- Enable **Hide options button** in order to remove the button for the **Options** menu from the logon window.
- Set the **Debug level** according to your requirements: 1 is the lowest level, 5 is the highest.

## 6.24. SSH Session

Menu path: **Setup > Sessions > SSH**

This section describes the procedure for configuring an SSH session.

Use the SSH session to launch a remote application on the host via SSH (Secure Shell) and display it on the terminal. SSH allows secure, encrypted communication between two hosts or host and terminal via an unsecured network. X11 connections can also be routed via this secure channel.

Command	All necessary entries for creating an executable command to remotely launch the application via SSH
User name (remote)	Name of the remote user - The selected user must have a user account on the remote host.
Computer (remote)	Name or IP address of the remote host from which the remote application is launched.
Command line	Allows you to enter the name of the application program which is to be launched.
Options	
Forward X11 connection	X11 connections are automatically forwarded to the remote computer so that each X11 program launched from the shell or the command passes through the encrypted SSH channel. The authentication data are also defined automatically. This option is enabled by default.
Enable compression	Reduces the amount of data transmitted via the data channel - This option is disabled by default.
Get protocol version	You must prove your identity to the remote host using one of the various identification methods. These depend on the protocol version used. In this area, you can obtain details of the protocol version after opting for a particular identification method.

➡ You will find detailed information on SSH and the various authentication methods on the relevant pages of the manual for your server operating system.

## 6.25. VNC Viewer

Menu path: **Setup > Sessions > VNC Viewer**

Create a **VNC Viewer session** in order to be able to access remote computers (VNC server) via the thin client. Connection options such as the server address or the full-screen mode can be pre-populated for each session or defined individually when the system starts.



If a server address is specified for the session, the connection dialog will not appear when the session starts – the connection will be established immediately.

## 6.26. VERDE session

Menu path: **Setup > Sessions > VERDE Sessions**

Virtual Bridges VERDE is a scalable virtual desktop solution. It supports traditional virtual desktop environments, available remote branches and both Windows and Linux users. VERDE is the basis for IBM Virtual Desktop.

➡ More information is available from Nimboxx.

## 6.27. Firefox browser

Menu path: **Setup > Sessions > Browser**

In order to allow central configuration via the IGEL UMS, the original configuration parameters for the Firefox 38.4.0 ESR web browser are assigned to the IGEL setup. These global settings can be changed for each browser session.

### 6.27.1. Browser Global

Menu path: **Setup > Sessions > Browser > Browser Global**

In this area, you can determine the browser start page, the display resolution and the font size.

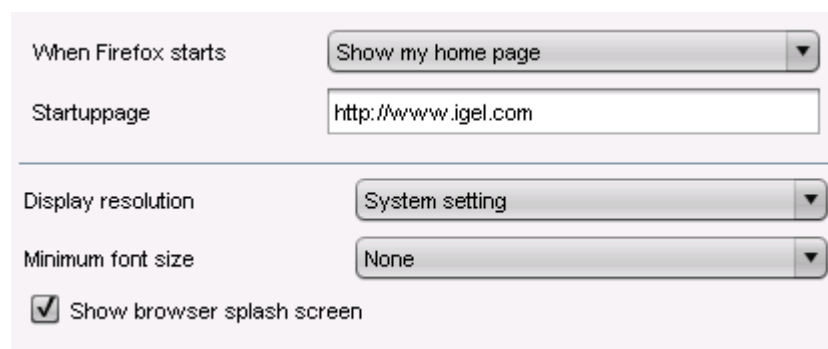


Figure 38: Settings under Browser Global

- Select an appropriate start screen from the following options:
  - Start with a blank page
  - Show my home page
  - Load the last visited page
  - Resume previous session
- Under **Startuppage**, specify the URL if you would like to launch Firefox with the home page.



To define a set of multiple home pages, separate the URLs with the "|" symbol.

- Select the desired **Display resolution** in DPI - e.g. 72 for medium-sized screens or 96 for large screens.
- Optionally, specify a **Minimum font size**.
- If necessary, disable **Show browser splash screen** – it is enabled by default.

## Tabs

Menu path: **Setup > Sessions > Browser > Browser Global > Tabs**

In this area, you determine the settings which affect the individual tabs in the browser.

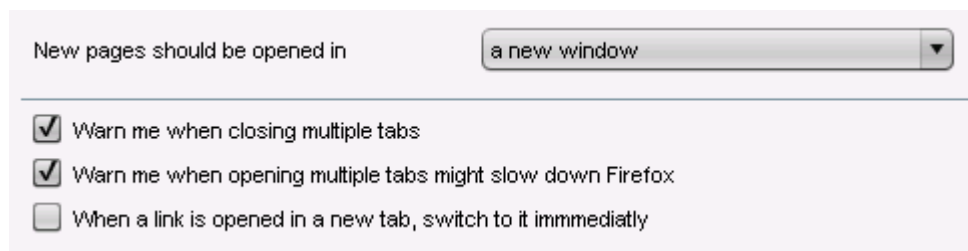


Figure 39: Tabs settings

- Select whether a new **browser page** is to be opened in the current browser window, in a new browser window or in a new tab.

By default, you are warned if you close a number of tabs at the same time or if too many tabs are open and this is slowing down browser performance.

- Uncheck the relevant checkboxes to disable the warnings.

By default, tabs which are opened from the left open in the foreground.

- Uncheck the **When a link is opened in a new tab, switch to it immediately** checkbox in order to open these tabs in the background.

## Contents

Menu path: **Setup > Sessions > Browser > Browser Global > Content**

In this area, you can define all settings which affect pop-up windows and downloads.

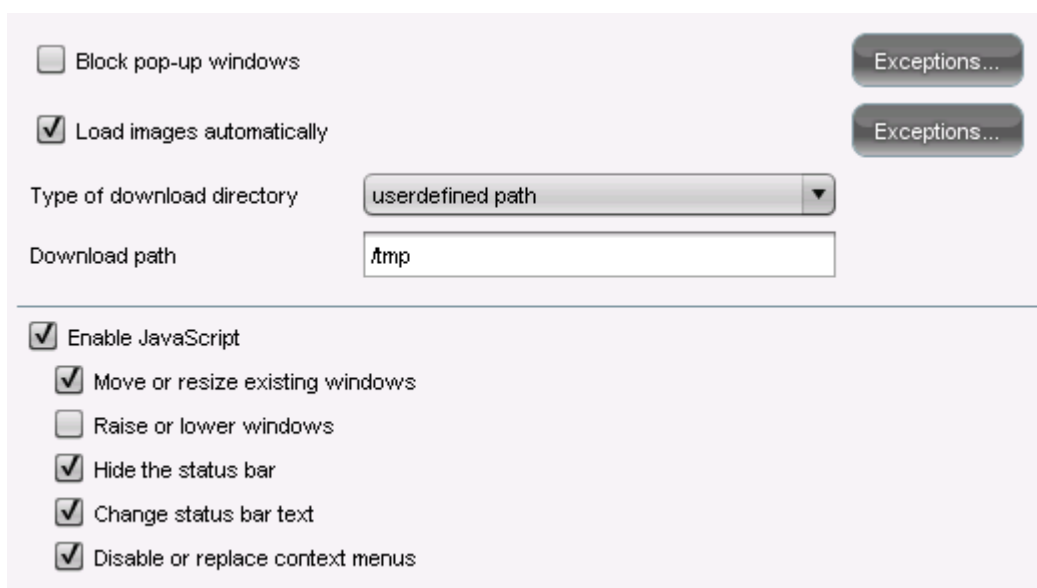


Figure 40: Browser content settings

**Block pop-up windows** is enabled by default.

- Uncheck the checkbox in order to allow pop-ups when loading pages.



- Specify **exceptions** in order to exclude specific pop-ups from the setting.

**Load images automatically** is enabled by default.

- Uncheck the checkbox in order to prevent images being loaded automatically. This will allow browser pages to load more quickly. Here too, you can define **exceptions**.

The **download directory** can be defined here. If you select **User-defined path**, the exact path must be given.



For reasons of space, you should not use a local path.

**Enable JavaScript** is enabled by default. The exact settings can be defined here.

- Uncheck the checkbox in order to disable JavaScript.

## Print

Menu path: **Setup > Sessions > Browser > Browser Global> Print**

In this area, you can set the **default paper size** for the printer.

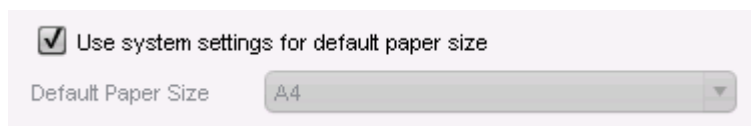


Figure 41: Paper size setting

## Proxy

Menu path: **Setup > Sessions > Browser > Browser Global> Proxy**

In this area, you can select the proxy configuration. You have four options:

<b>Direct connection to the Internet</b>	Enable this option if you do not wish to use a proxy.
<b>Manual proxy configuration</b>	<p>Configure the proxy individually.</p> <p>Under <b>No proxy for</b>, you can list entries for which no proxy will be used, e.g. <code>.mozilla.org</code>, <code>.net.de</code>, <code>.net.nz</code>.</p> <p>Under Proxy realm, give details of the area for which the proxy is responsible. This information must be provided in order for automatic logon to work.</p> <p>Leave the <b>Proxy realm</b>, <b>User name</b> and <b>Password</b> boxes empty in order to allow manual entries when logging on.</p>
<b>Automatic proxy configuration</b>	Specify the <b>URL</b> for automatic proxy configuration.
<b>System-wide proxy configuration</b>	Use the network/proxy settings from the IGEL setup.

☒ Direct Connection to the internet  
☐ Manual proxy configuration

---

FTP Proxy  Port   
 HTTP Proxy  Port   
 SSL Proxy  Port   
 SOCKS Host  Port   
 SOCKS Protocol version

No Proxy for

☒ Automatic proxy configuration URL   
☐ Systemwide proxy configuration

Figure 42: Proxy settings

## Data protection

Menu path: **Setup > Sessions > Browser > Browser Global> Privacy**

Here, you can configure data protection settings for the following areas:

- *Private data* (page 82)
- *Protection against tracking* (page 83)
- *Browser address bar* (page 84)

## Private data

Menu path: **Setup > Sessions > Browser > Browser Global> Privacy**

In this area, you can define settings for your browsing history and private data.

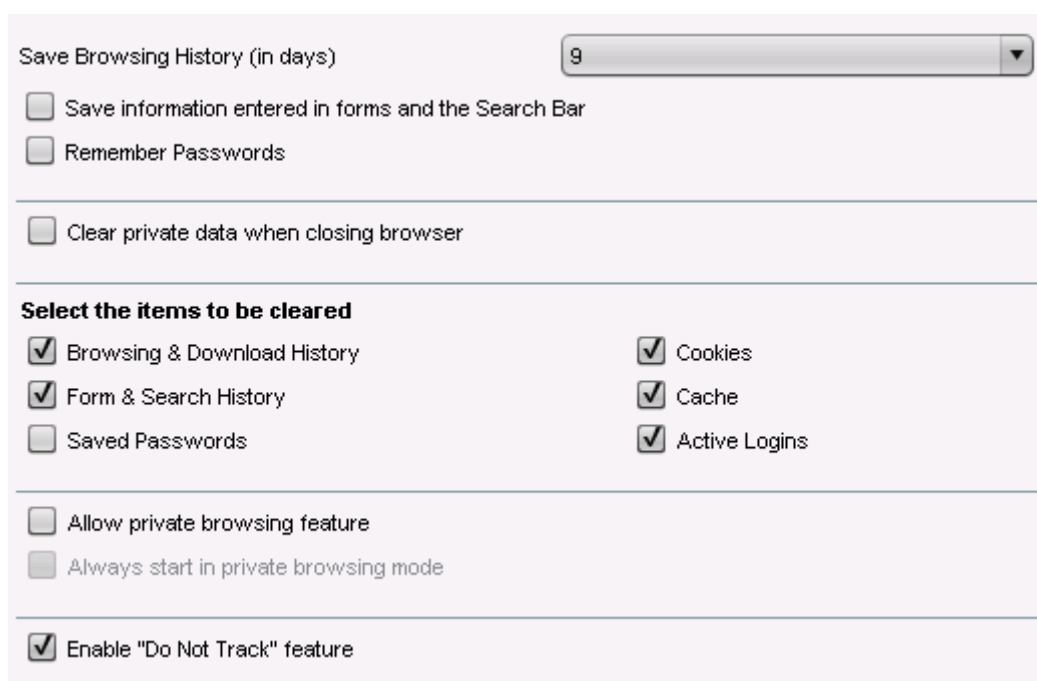


Figure 43: Data protection settings

- Define whether, and if so, in how many days you would like to save your **browsing history**.



Any history created before the defined date will be lost when you restart your browser.

- Define whether you would also like to save **entries in forms and search bars** or **passwords** in your history.
- Enable **Clear private data when closing browser** if you would like to delete at the end of the browser session the data created when surfing.
- Specify exactly which private data you would like to delete.
- Enable **Allow private browsing feature** in order to use Firefox in private mode where no data are stored.
- Enable **Launch browser in private mode as standard** if Firefox should always start in private mode.

## Protection against tracking

Menu path: **Setup > Sessions > Browser > Browser Global > Privacy**

In this area, you can specify how you would like to protect yourself against tracking on the Internet.

- ☒ Enable "Do Not Track" feature
- ☒ Enable built-in tracking protection

Figure 44: Do not track

- Disable the **Do not track feature** if you would like to allow websites to track your activities.



The **Do not track (DNT) feature** is enabled by default. With this function, you tell a website that you do not want to be tracked by third parties, e.g. for behavioral advertising. Do not track transfers an HTTP header every time that you request data from the Internet. In this case, the site visited decides what it will do with the privacy request.

- Disable **tracking protection** if you do not wish to use the tracking protection provided by Firefox.



With protection against the tracking of activities, you can control your online privacy. Even if Firefox includes a **do not track feature** which tells websites that you do not want your surfing habits to be recorded, companies do not have to adhere to it. The protection against tracking in Firefox puts you in control by blocking domains and websites which are known for tracking users. In this case, Firefox actively blocks content which records the user's surfing habits.

## Address bar

Menu path: **Setup > Sessions > Browser > Browser Global > Privacy**

Here, you can specify further rules in order to tailor the behavior of the address bar to your needs:

- ☒ Suggest visited sites in URL bar
  - ☐ Suggest only typed visited sites
- ☒ Suggest bookmarked sites in URL bar
- ☒ Suggest open pages in URL bar

Figure 45: Further data security settings

- When typing in a URL, would you like to be given suggestions from **history entries**? Or only from entries that you actually typed in?
- Or would you like to be given suggestions from your **bookmarks**?
- Should **tabs that were previously opened** be suggested as a destination?

## Security

Menu path: **Setup > Sessions > Browser > Browser Global > Security**

In this area, you can define settings for phishing and malware.

**Safe browsing** is disabled by default.

- Check the checkbox in order to enable integrated phishing protection.

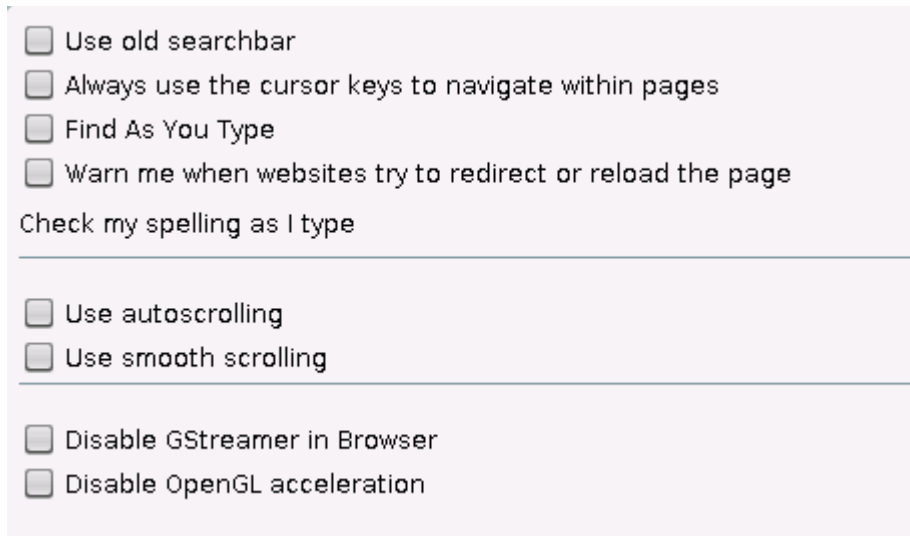
**Malware protection** is disabled by default.

- Check this checkbox in order to download malware blacklists and check downloads for malware.

## Advanced

Menu path: **Setup > Sessions > Browser > Browser Global> Advanced**

In this area, you can define settings for entry options, scrolling and websites.



<input type="checkbox"/> Use old searchbar
<input type="checkbox"/> Always use the cursor keys to navigate within pages
<input type="checkbox"/> Find As You Type
<input type="checkbox"/> Warn me when websites try to redirect or reload the page
Check my spelling as I type

---

<input type="checkbox"/> Use autoscrolling
<input type="checkbox"/> Use smooth scrolling

---

<input type="checkbox"/> Disable GStreamer in Browser
<input type="checkbox"/> Disable OpenGL acceleration

Figure 46: Advanced settings

- Enable **Always use the cursor keys to navigate within pages** if you would like to use this function.
- Enable **Find as you type** if you would like to see search suggestions while typing.
- Enable **Warn me when websites try to redirect or reload the page** if you would like to use this function.
- Select **Check spelling as I type** and specify whether you would like this to apply to text fields only or to text fields and text lines.
- If you select **Use autoscrolling**, you can move the view of a website in the display area vertically by pressing the middle mouse button and moving the mouse.
- Select **Use smooth scrolling** in order to scroll line by line or pixel by pixel.
- Enable **Disable GStreamer support for the browser** if you have problems when playing back videos on HTML5 websites.
- Enable **Disable OpenGL acceleration** if your client has problems with OpenGL applications.

## Encryption

Menu path: **Setup > Sessions > Browser > Browser Global> Encryption**

In this area, you can determine the settings for encryption protocols, certificate validation and authentication solutions.

## Encryption



Minimum required encryption protocol	SSL3
Maximum supported encryption protocol	TLS 1.2
When a website requires a certificate	Select one automatically

Figure 47: Encryption settings

- Select a minimum and maximum **encryption protocol**. The following are available to choose from
  - SSL3
  - TLS 1.0
  - TLS 1.1
  - TLS 1.2
- Determine what is to be done **if a website asks for a security certificate**.
- Click on **Show certificates** in order to manage the certificates used by Firefox.

## Certificate validation



Certificate Validation (Online Certificate Status Protocol)	Validate a certificate if it specifies an OCSP server
Response Signer	Builtin Object Token:IPS CLASE1 root
Service URL	http://ocsp.ips.es/
<input type="checkbox"/> When an OCSP server connection fails, treat the certificate as invalid	

Figure 48: Certificate settings

- Define the **Certificate validation**. The following are available to choose from:
  - Validate a certificate if it specifies an OCSP server
  - Do not use OCSP for certificate validation
  - Validate all certificates using the following OCSP server

In this case, you will need to give details of the **response signer** and the **service URL**.

If you have selected validation with OCSP, you can enable the **When an OCSP server connection fails, treat the certificate as invalid** option.

## Authentication

- Select an authentication solution from the following products in order to protect your network:



A list of authentication solutions, each preceded by an unchecked checkbox:

- ☐ Use "Aladdin eToken" Security Device
- ☐ Use "Gemalto" Security Device
- ☐ Use "IDProtect" Security Device
- ☐ Use "SafeSign" Security Device
- ☐ Use "SecMaker" Security Device
- ☐ Use TCOS 3 NetKey Security Device
- ☐ Use TCOS 3 SigG Security Device
- ☐ Use TCOS 3 Elster Security Device
- ☐ Use TCOS 3 SD Security Device

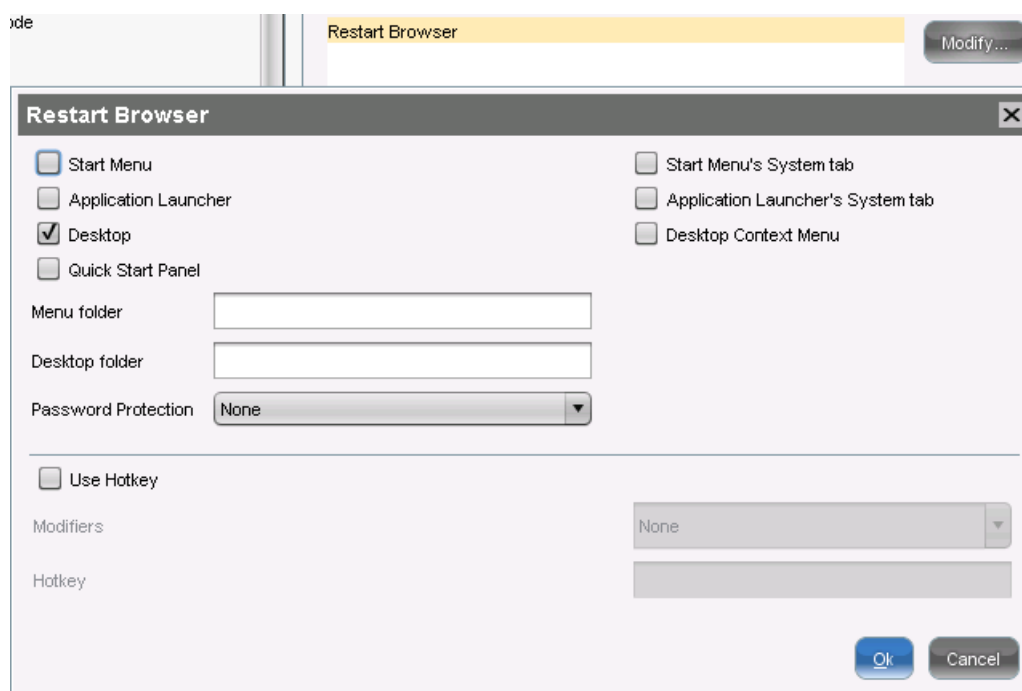
Figure 49: Authentication solutions

## Commands

Menu path: **Setup > Sessions > Browser > Browser Global > Commands**

In this area, you can specify the settings for certain commands.

- Click on a command in order to enable the **Edit** button.



The screenshot shows the 'Restart Browser' dialog box. At the top, there is a tab labeled 'Restart Browser' and a 'Modify...' button. The dialog box contains the following settings:

- ☐ Start Menu
- ☐ Application Launcher
- ☒ Desktop
- ☐ Quick Start Panel
- ☐ Start Menu's System tab
- ☐ Application Launcher's System tab
- ☐ Desktop Context Menu
- Menu folder:
- Desktop folder:
- Password Protection:
- ☐ Use Hotkey
- Modifiers:
- Hotkey:

At the bottom right, there are 'Ok' and 'Cancel' buttons.

Figure 50: Commands setting

## 6.27.2. Firefox Browser Session

Menu path: **Setup > Sessions > Browser > Browser Sessions**

The original Firefox parameters are pre-set under **Settings**. The standard settings are carried over from the **Browser Global** setup.

The following settings for the browser session can also be configured:

Window	Allows you to specify the full-screen mode and multi-monitor options as well as the Firefox language / prevent users making changes to the browser / hide the configuration page (about:config) and the printer dialog
Symbol bars and toolbar	Allows you to hide/show toolbar items or complete toolbars in a session / configure a kiosk mode (browser in full-screen mode, restricted access to toolbars and autostart/restart configuration)
Hotkeys	Allows you to enable/disable hotkeys used in the Firefox browser.
Context menu	Allows you to enable/disable items in the browser context menu.

### Window settings

Menu path: **Setup > Sessions > Browser > Browser Sessions > Window**

In this area, you can define the window settings for a browser session.

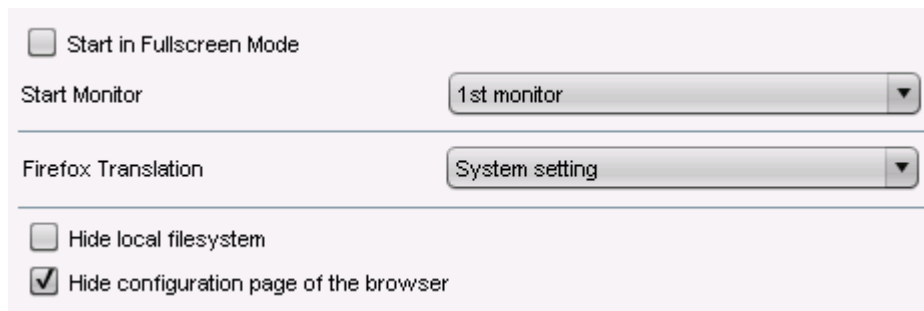


Figure 51: Window settings

The **full-screen mode** is disabled by default.

- Check the checkbox in order to enable the full-screen mode.

If you have connected a number of monitors, you can specify the **start monitor** here.

- Under **Firefox translation**, select the language that the Firefox user interface is to be translated into.
- Enable **Hide local file system** if you do not want the local structure to be displayed when you save files.
- Disable **Hide configuration page of the browser** if you would like the configuration page of the browser to be displayed for editing.



## Menus and symbol bars

Menu path: **Setup > Sessions > Browser > Browser Sessions > Menus & Toolbars**

In this area, you can adapt Firefox menus and symbol bars to meet your personal needs by

- Hiding items in the menu bar
- Hiding list items
- Configuring the symbol bar

➤ Enable **User customization of tool bars** in order to allow the user to configure symbol bars.

➤ Configure the **navigation symbol bar**.

The following items are pre-set:

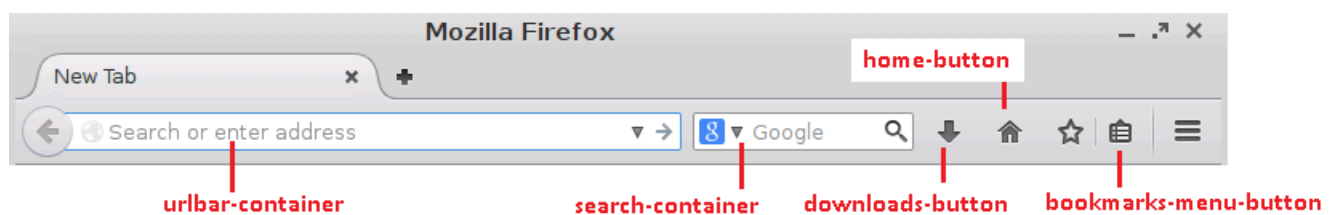


Figure 52: Navigation symbol bar

➤ Configure the **Application menu**:

The following items are pre-set:

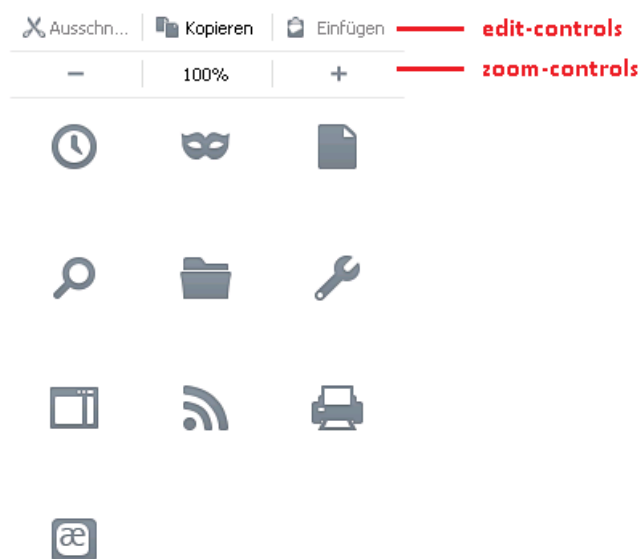


Figure 53: Application menu



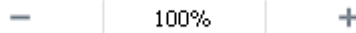
Please note that a number of items are only shown if the corresponding feature is enabled.

- Configure the **Application menu**:
- **Other possible items for the navigation symbol bar and the application menu are:**

Loop button



Zoom controls



Edit controls



History panel menu



Private browsing button



Save page button



Find button



Open file button



Developer button



Sidebar button



Feed button



Print button



Character encoding button



Social share button



Panic button



Web apps button



New window button



Fullscreen button



Tab view button



Downloads button



- Click on **Reset icon configuration to default** in order to undo your changes.

## Hotkeys

Menu path: **Setup > Sessions > Browser > Browser Sessions > Hotkeys**

In this area, you can disable the following Firefox hotkeys:

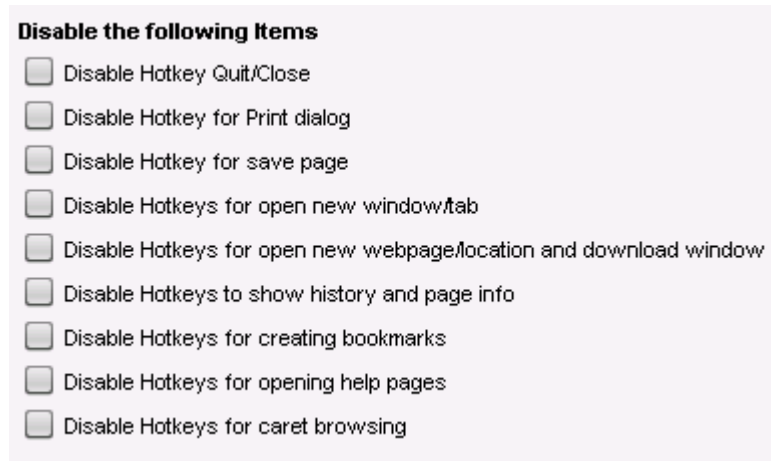


Figure 54: Hotkeys settings

## Context menu

Menu path: **Setup > Sessions > Browser > Browser Sessions > Context**

In this area, you can disable various items in the browser context menu.

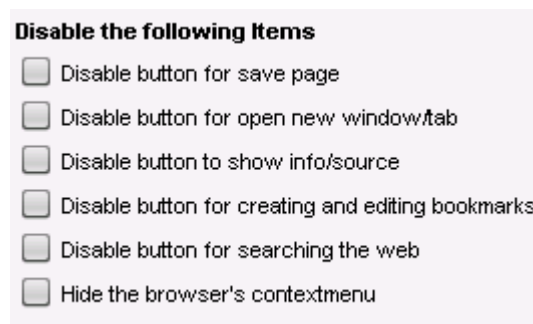


Figure 55: Context menu settings

### 6.27.3. Browser Plug-ins

Menu path: **Setup > Sessions > Browser > Plugins**

Various plug-ins such as a PDF viewer, Adobe Flash Player or Red Hat Spice are available. However, they may need to be licensed by the user first. Integration of the SecMacer security solution Net iD can also be configured here.

## Flash Player

Menu path: **Setup > Sessions > Browser > Plugins > Flashplayer**

Before you can download and install Adobe Flash Player, you need to confirm that the software is licensed - IGEL Universal Desktop Linux does not contain a license to use the Flash Player.

➤ Activate the option **I will license the flashplayer by myself** to activate the **Download Flashplayer** page.

To install Adobe Flash Player:



You can also start the installation using the UMS context menu. For this, select **Other Thin Client commands > Download Flashplayer** in the context menu.

1. Navigate to the **Download Flashplayer** page.
2. Activate the option **I want to download Adobe flashplayer and care about the licensing by myself**.
3. Adjust the following settings:
  - **Use Firmware Update settings for download:** If the option is activated, the parameters **User authentication**, **User name**, **Password**, and **Download URL** are set to the default values and cannot be changed.
  - **User authentication:** If the option is activated, the thin client authenticates with the server using the access data provided in **User name** and **Password**.
  - **Download URL:** URL of the directory in which the Adobe Flash Player is stored. The default value is the official link from Adobe. Alternatively, you can provide the storage location in your company network.



The Adobe link is valid at the time when the firmware is released, but it is subject to change. In case the download fails, modify the URL accordingly.

- **Download File:** Name of the file containing the Adobe Flash Player.
1. Click **Apply** or **Ok**.

The Adobe Flash Player is downloaded and installed.

## PDF viewer

Menu path: **Setup > Sessions > Browser > Plugins > PDF Viewer**

Here, you can specify whether PDF documents are to be embedded in the browser or displayed in a separate window.

## RedHat Spice

Menu path: **Setup > Sessions > Browser > Plugins > RHEV/Spice**

In this area, you can define settings for virtual environments.

- Enable **Enable browser plugin** in order to display virtual desktop environments everywhere via the Internet.
- Enable or disable **Enable USB sharing**.

## 6.28. Media Player

Menu path: **Setup > Sessions > Media Player**

Set up the Media Player for your multimedia applications here.

IGEL Linux supports the following multimedia formats and codecs out of the box:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC

The following codecs are licensed via the separately available Multimedia Codec Pack:

Supported formats:	Supported codecs:
AVI	MP3
MPEG	WMA stereo
ASF (restricted under Linux)	WMV 7/8/9
WMA	MPEG 1/2
WMV (restricted under Linux)	MPEG4
MP3	H.264
OGG	



AC3 is not licensed.



IGEL Zero Clients (IZ series) have the Multimedia Codec Pack installed by default.

### 6.28.1. Media Player Global

Menu path: **Setup > Sessions > Media Player > Media Player Global**

➤ Configure universal settings which will apply by default during all Media Player sessions.



You can override global settings in the individual sessions.

## Window

Menu path: **Setup > Sessions > Media Player > Media Player Global > Window**

- Under **Image Aspect Ratio**, specify the required aspect ratio for video playback.

You can also choose the following options:

- Full-screen mode
- Automatically change window size as soon as a new video is loaded
- Main window should remain in the foreground
- Show operating components

## Playback

Menu path: **Setup > Sessions > Media Player > Media Player Global > Playback**

- Specify how you would like to play back media files:

<b>Endless loop</b>	Automatically plays back a play list endlessly until you stop it.
<b>Random mode</b>	Plays back the files in a play list in a random order.

- If you wish, choose the visual effects to be used during audio playback.

<b>Visualization type</b>	Determines the visualization plug-in.
<b>Visualization size</b>	Determines the visualization size.

## Video

Menu path: **Setup > Sessions > Media Player > Media Player Global > Video**

<b>Video output</b>	GConf:	System-wide configuration
	Auto:	Automatically selects the output
	XVideo:	Hardware-accelerated, uses shared memory to write images to the graphics card memory
	X11:	Not hardware-accelerated, playback via the X Window System display protocol

- Specify the brightness, saturation, contrast and color settings for videos.

## Audio

Menu path: **Setup > Sessions > Media Player > Media Player Global > Audio**

<b>Audio output</b>	GConf:	System-wide configuration
	Auto:	Automatically selects the output
	ALSA:	Direct output via kernel driver for sound cards

**Audio output type**

Select Stereo if you are working with an IGEL thin client.

## Options

Menu path: **Setup > Sessions > Media Player > Media Player Global > Options**

- Specify whether you would like to disable the **screen saver** during audio playback.
- Specify the **network connection speed** in order to influence media file playback.
- Specify the necessary **buffer size** for your network in order to ensure smooth audio and video playback.
- Specify whether you would like to **automatically load subtitles** as soon as a video begins. Currently, the **coding** for subtitles is always UTF-8.
- Specify the **font** and **text size** for the subtitles.

## Browser Plugin

Menu path: **Setup > Sessions > Media Player > Media Player Global > Browser Plugin**

If you would like to use the Media Player as a **Browser Plugin**, you can change the configuration values here.



This will affect manually configured Media Player sessions.

### 6.28.2. Media Player Sessions

Menu path: **Setup > Sessions > Media Player > Media Player Sessions**

You can set up your own personal Media Player sessions here.

1. Click on **Add** to create a new session.
2. Specify a **session name**.
3. Specify which **possible ways of launching the session** you would like. You may choose a number of options here.
4. You may like to select the option of using **hotkeys** and define them.
5. You can also specify whether **autostart** (following a system start) and/or **restart** (after a connection is established) are to be used.
6. For the autostart option, you can also specify by how many seconds the session start is to be delayed.

As soon as you have set up a Media Player session of your own, it will appear in the structure tree under the **Media Player Sessions** directory. Your own session in turn contains three folders: **Playback**, **Options** and **Desktop Integration**.



## Playback

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session name] > Playback**

- Under **Medium / File**, give the path of the file which is to be played back when the session is launched. Use the following formats:

`/directory/filename`

or

`http://servername/filename.`

For the window settings, you can choose whether you would like to carry over the global settings or use your own settings for this special session.

## Options

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session name] > Options**

If necessary, you can change the pre-configured settings for the operating components here.

## 6.29. Java Web Start Session

Menu path: **Setup > Sessions > JWS Sessions**

In order to be able to access Java Web Start (JWS) applications, enter the address of the necessary JNLP file. For example, this may be an IGEL UMS console which can also be run as a Java Web Start application.

## 6.30. VoIP Client

Menu path: **Setup > Sessions > VoIP Client**

This section describes the procedure for setting up voice-over IP telephony (VoIP). The IGEL Universal Desktop Linux firmware includes the Ekiga voice-over IP client (<http://ekiga.org>). This client allows you to use the SIP (Session Initiation Protocol) and H.323. In addition to the local contact list, the telephone book can also search the LDAP address books.

- ➡ You will find a detailed description of all Ekiga options under <http://wiki.ekiga.org/index.php/Manual>.

## 7. Accessories

Menu path: **Setup > Accessories**

Information on other accessories provided by the Universal Desktop can be found [here](#).

### 7.1. ICA Connection Center

Menu path: **Setup > Accessories> ICA Connection Center**

The Citrix ICA Connection Center provides an overview of existing connections to Citrix servers. It also allows the server connection to be terminated/canceled and the connection properties to be displayed, e.g. for support purposes.

### 7.2. Local Terminal

Menu path: **Setup > Accessories> Terminals**

With a terminal session, you can execute local commands via a shell.



It is also possible to access a local shell without a terminal session: You can switch to the virtual terminals tty11 and tty12 by pressing **Ctrl+Alt+F11** / **Ctrl+Alt+F12**.

### 7.3. Change Smartcard Password

Menu path: **Setup > Accessories> Change Smartcard Password**

Set up a session in order to change your IGEL smartcard password. Details of the setup procedure for your IGEL smartcard can be found under **Security > Login > Smartcard**.

### 7.4. Setup Session

Menu path: **Setup > Accessories> Setup**

Specific areas of the setup can be made available to the user, even if the overall setup can only be accessed by the administrator. This is useful for example for keyboard and mouse settings or for screen configuration. See *Enable Setup Pages for Users* (page 21).

## 7.5. Quick Settings Session

Menu path: **Setup > Accessories > Quick Setup**

Specific areas of the setup can be made available to the user, even if the overall setup can only be accessed by the administrator. This is useful for example for keyboard and mouse settings or for screen configuration. See Quick Setup.

## 7.6. Display switch

Menu path: **Setup > Accessories > Display Switch**

Display switch is a function of the IGEL Linux firmware which allows you to configure settings for the display on various screens.

In order to use the function, you will need to enable it and set it up:

- Enable screen selection by enabling one of the **session launching options** under **Accessories > Display Switch**.
- Enable **Use hotkeys** in order to determine a hotkey or an icon for this session.
- If necessary, specify **autostart options**.
- Configure the following settings under **Accessories > Display Switch > Options**:

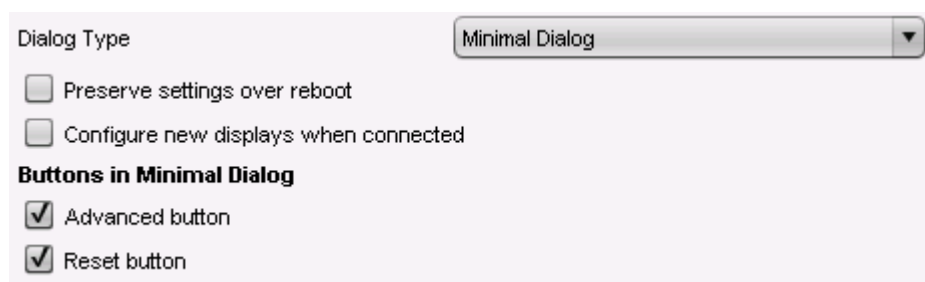


Figure 56: Settings for switching displays

- Under **Dialog Type**, specify how the screen selection dialog is to look:
  - **Minimal Dialog** - Basic settings such as **Mirror** or **Expand**, for a maximum of two displays.
  - **Advanced Dialog** - The user themselves can change the resolution or rotation outside the setup.
- Enable **Preserve settings over reboot** in order to preserve the configuration carried out.



This setting has no function under the following condition: You work with **Shared Workplace** and have assigned profiles to various users via the UMS. You can save the default settings for users who are not assigned a profile. With the other users, these settings will be overwritten by the profile from the UMS.

- Enable **Configure new displays when connected** in order to be able to configure settings for newly connected devices.

As soon as you connect a new display, a configuration window will open.

- Enable **Preserve settings over reboot** in order to save the display settings so that they can be reused in the event of a reboot.
- Specify the buttons for the minimal dialog:
  - **Advanced button** - Allows you to jump to the advanced dialog in the minimal dialog.
  - **Reset button** - Allows resetting to the setup settings in the dialog.

### 7.6.1. Advanced settings

Menu path: **Setup > Accessories > Display Switch > Options**

To set up your screens' **Display**, proceed as follows:

1. Open the **Display Switch** that you set up under **Display Switch** (page 99).

The **Displays** mask will open.

2. Click on **Advanced** in order to be able to configure special display options.

The **Display** mask will open:

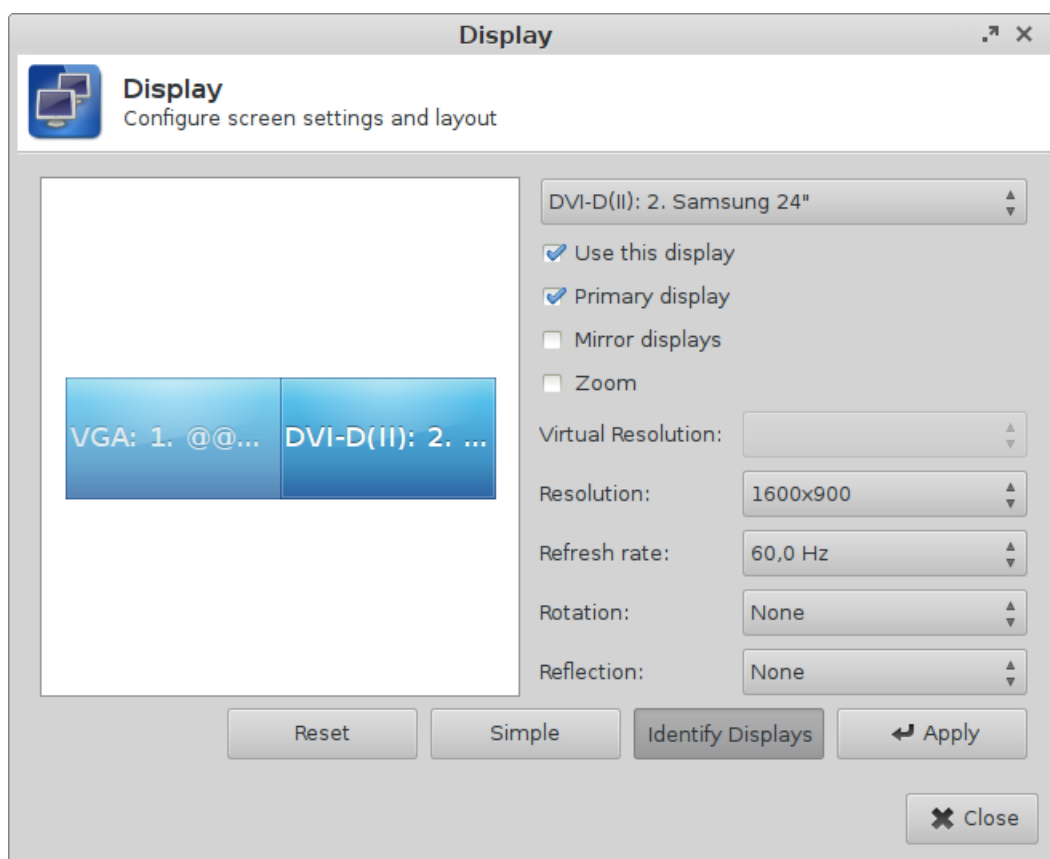


Figure 57: Magnified view

Click on one of the screens shown and configure the settings, e.g.:

- **Use this display** - in order to enable it.
- **Primary display** - in order to specify the first screen, see **Screen 1** in the *Screen Selection* (page 116). The taskbar appears on the main screen.
- **Mirror displays** - in order to place the screens over each other.
- **Zoom** - in order to set the magnified display.



If you disconnect the only active screen, the one that was active last will be shown again. As a result, you can still configure something even in an emergency.

### 7.6.2. Magnified view

You have the option of displaying a magnified setup interface on your screen. This was developed for users with impaired vision.

1. Activate **Zoom** in the **Display** (page 100) window.

The **Virtual Resolution** selection field will become active.

Figure 58: Set resolutions



Under **Virtual Resolution** and **Resolution**, the current resolution value is preset as the default value.

2. Configure the following settings for the magnification function:
  - Under **Virtual Resolution**, select the highest possible value from the selection list.
  - Under **Resolution**, select a much lower value which should simulate the actual resolution of the screen.

The setup interface is now shown as if it would fill a much larger screen. The existing screen thus shows just part of the interface. Essentially, it functions like a magnifying glass or a peephole. The part of the interface that can be seen is highly magnified.



If you selected **Mirror Displays** under the advanced settings, all active screens will be displayed in the same way. They basically lie over each other. However, you can change the way they are displayed in magnification mode by reducing the actual resolution of the mirrored screen.

## 7.7. Application Launcher

Menu path: **Setup > Accessories > Application Launcher**

- Show the **Setup** and **Application Launcher** on the local desktop or in the start menu, or define hotkeys and the autostart option.

You can hide various items, e.g. buttons for shutting down or restarting the device, from the user.

## 7.8. Sound Mixer

Menu path: **Setup > Accessories > Sound Preferences**

Use the sound control to adjust the output volume and the input level as well as the balance between the input and output.

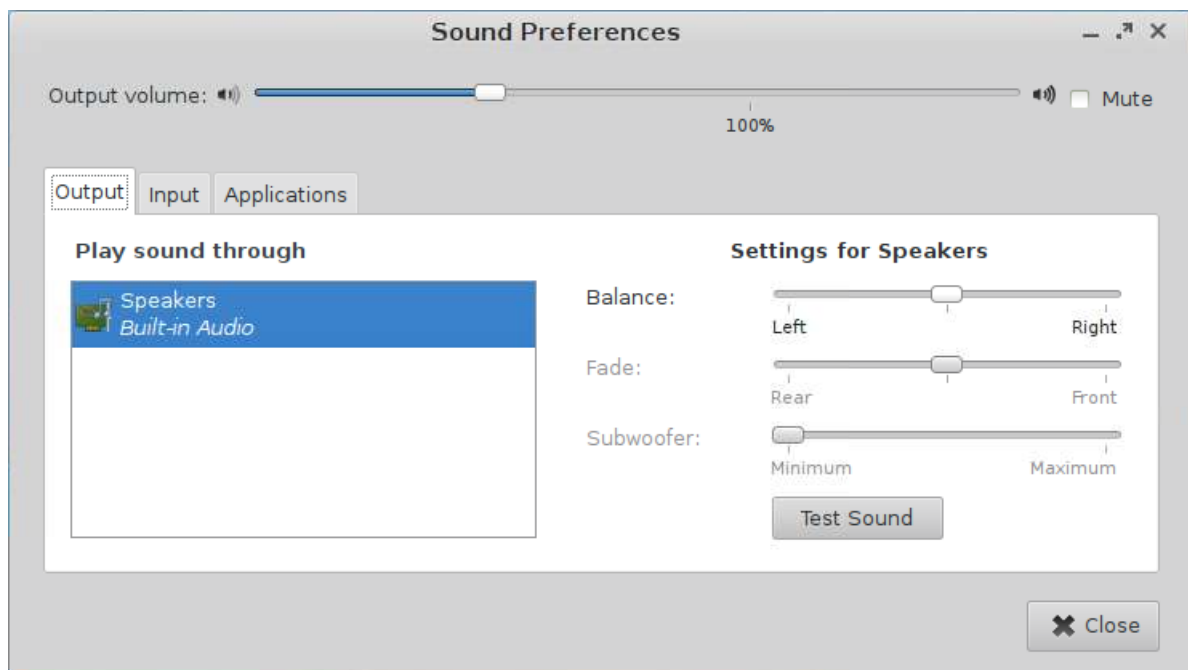


Figure 59: Sound control

The system's default volume can be configured or muted in **Accessories > Sound Mixer > Configuration**. These parameters can also be remotely set via IGEL UMS.

## 7.9. System Log Viewer

Menu path: **Setup > Accessories > System Log Viewer**

All available system logs are updated and displayed. You can add your own log files in the options. The contents of the selected log can be searched in the viewer and also copied (e.g. for support purposes).

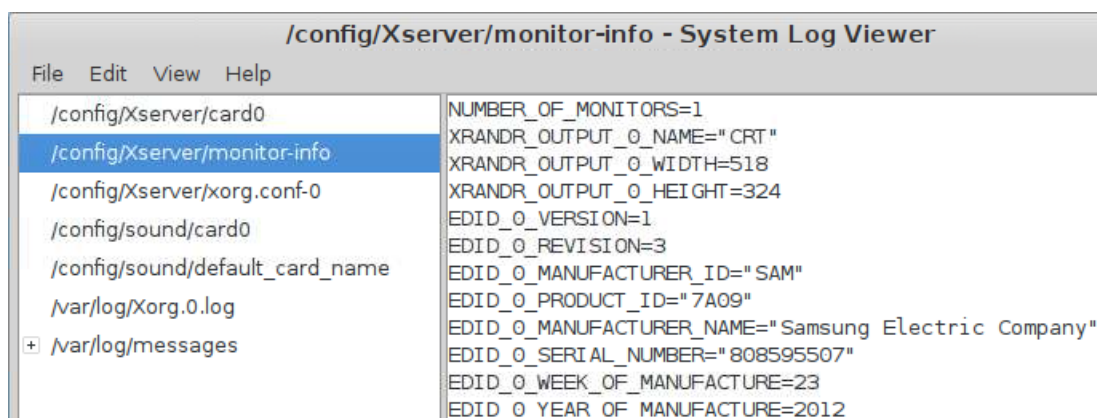


Figure 60: System logs

## 7.10. UMS Registration

Menu path: **Setup > Accessories > UMS Registering**

Registration of the thin client in the IGEL Universal Management Suite can also be performed locally. To do this, enter the server address (with port) and the necessary access data. Directories already on the server can be selected directly.

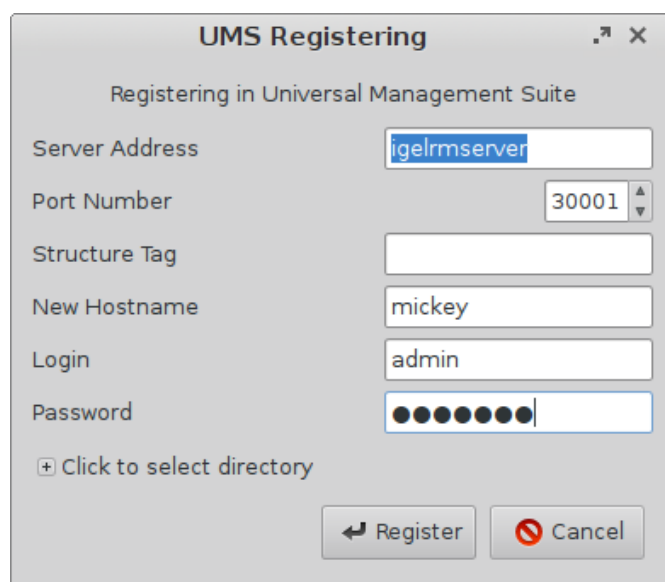


Figure 61: Register thin client on the UMS Server

## 7.11. Touchscreen calibration

Menu path: **Setup > Accessories > Touchscreen Calibration**

Enable the calibration program for your touchscreen here and specify how you would like to bring it up.

After launching the calibration program, you will see a pattern with calibration points which must be touched one after another.

➡ Further settings options can be found under Touchscreen.

## 7.12. Task Manager

Menu path: **Setup > Accessories > Taskmanager**

This function provides an overview of the applications and other processes running on the thin client.

Information regarding use of this function can be found under *Using the Task Manager* (page 105). The settings for launching the function are described below.

- To apply a changed setting, click on **Apply**.
- To apply a changed setting and close the setup, click on **OK**.

You can change the following settings:

- **Session Name:** Name for the **Taskmanager** function
- **Start Menu:** If this option is enabled, the Task Manager can be launched in the start menu.
- **Application Launcher:** If this option is enabled, the Task Manager can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the Task Manager can be launched with a program launcher on the desktop.
- **Quick Start Panel:** If this option is enabled, the Task Manager can be launched in the Quick Start Panel.
- **Start Menu's system tab:** If this option is enabled, the Task Manager can be launched in the start menu's system tab.
- **Application Launcher's System tab:** If this option is enabled, the Task Manager can be launched in the Application Launcher's system tab.
- **Desktop Context Menu:** If this option is enabled, the Task Manager can be launched in the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the Task Manager. The menu path will be used in the start menu and in the desktop context menu. Example: "Functions/Screen functions".
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the Task Manager. The menu path will be used for the program launcher on the desktop. Example: "Functions/Screen functions".
- **Password Protection:** Specifies the password request when launching the Task Manager.

Possible values:



- **None:** No password is requested when launching the Task Manager.
- **Administrator:** The administrator password is requested when launching the Task Manager.
- **User:** The user password is requested when launching the Task Manager.
- **Setup user:** The setup user's password is requested when launching the Task Manager.
- **Hotkey:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the Task Manager.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the Task Manager will be launched automatically when the thin client boots
- **Restart:** If this option is enabled, the Task Manager will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the Task Manager being launched automatically.

### 7.12.1. Using the Task Manager

The following section explains how to use the Task Manager.

- Launch the **Task Manager** function. The launch options are described under *Task Manager* (page 104).

To determine the thin client's total processor usage, proceed as follows:

- Read the percentage value under **CPU**:



To determine the thin client's total memory usage, proceed as follows:

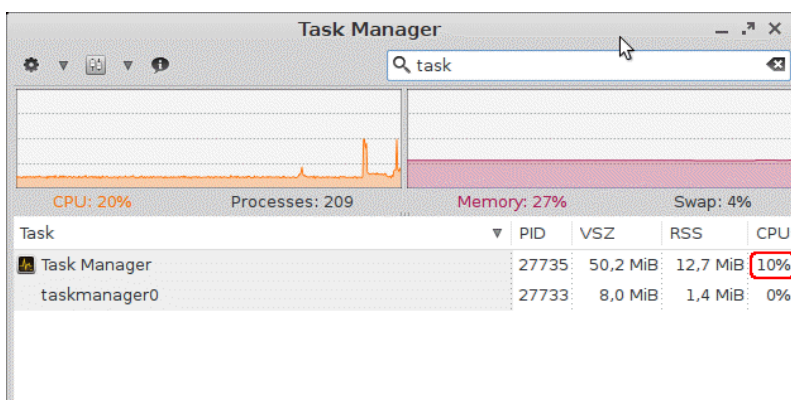
- Read the percentage value under **RAM**:



- To determine the value in bytes, click on  and enable the **Show memory usage in bytes** option.

To determine the extent to which a specific application contributes to processor usage, proceed as follows:

1. In the search window, enter the name of the application or part of the name.  
The Task Manager will now show only the relevant applications and processes.
2. Read the percentage value for the relevant application in the **CPU** column.



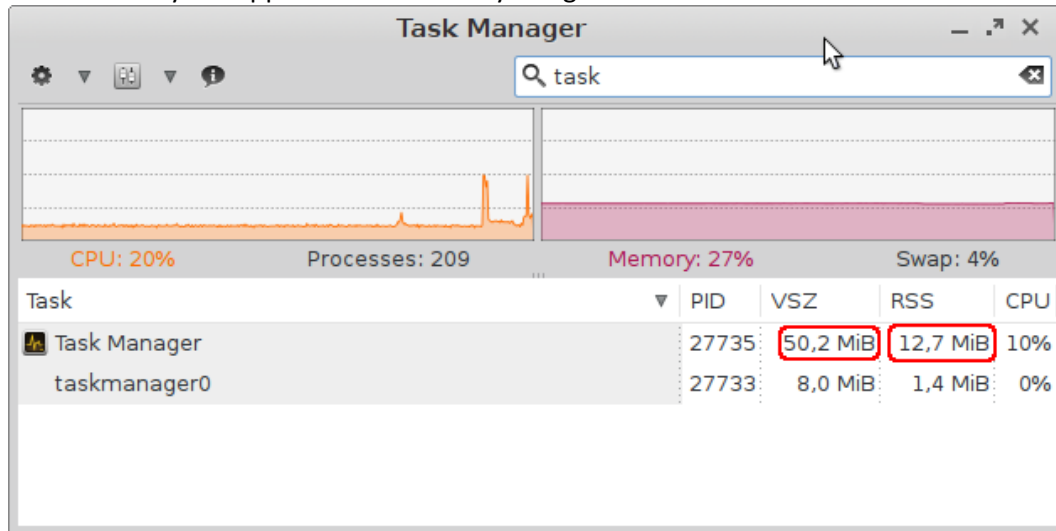
To determine the extent to which a specific application contributes to memory usage, proceed as follows:





1. In the search window, enter the name of the application or part of the name.

The Task Manager will now show only the relevant applications and processes.

2. Read the values in the **VSZ** and **RSS** columns.

The **VSZ** column shows how much memory is available for the application. The **RSS** column shows how much memory the application is currently using.



- If the **VSZ** column is not shown, click next to  on  and enable the **Virtual Bytes** option.
- If the **RSS** column is not shown, click next to  on  and enable the **Private Bytes** option.

## 7.13. Screenshot tool

Menu path: **Setup > Accessories > Screenshot Tool**

With this function, you can take a screenshot.

Information regarding use of this function can be found under *Taking a screenshot* (page 107). The settings for launching the function are described below.

- To apply a changed setting, click on **Apply**.
- To apply a changed setting and close the setup, click on **OK**.

You can change the following settings:

- **Session Name:** Name for the **Screenshot Tool** function.
- **Start Menu:** If this option is enabled, the **Screenshot Tool** function can be launched from the start menu.
- **Application Launcher:** If this option is enabled, the **Screenshot Tool** function can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the **Screenshot Tool** function can be launched with a program launcher on the desktop.
- **Quick Start Panel:** If this option is enabled, the **Screenshot Tool** function can be launched from the Quick Start Panel.
- **Start Menu's System tab:** If this option is enabled, the **Screenshot Tool** function can be launched in the start menu's system tab.
- **Application Launcher's System tab:** If this option is enabled, the **Screenshot Tool** function can be launched in the Application Launcher's system tab.
- **Desktop Context Menu:** If this option is enabled, the **Screenshot Tool** function can be launched in the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the **Screenshot Tool**. The menu path will be used in the start menu and in the desktop context menu. Example: "Functions/Screen functions".
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the **Screenshot Tool**. The menu path will be used for the program launcher on the desktop. Example: "Functions/Screen functions".
- **Password Protection:** Specifies the password request when launching the **Screenshot Tool** function.

Possible values:

- **None:** No password is requested when launching the **Screenshot Tool** function.
  - **Administrator:** The administrator password is requested when launching the **Screenshot Tool** function.
  - **User:** The user password is requested when launching the **Screenshot Tool** function.
  - **Setup user:** The setup user's password is requested when launching the **Screenshot Tool** function.
  - **Hotkey:** Specifies a hotkey which can be used to launch the **Screenshot Tool** function.
- ➡ You can also define a hotkey for taking a screenshot under **Setup > User Interface > Hotkeys > Commands**, see *Hotkeys* (page 140).
- **Modifiers:** Combination of modifiers for the hotkey. You can specify a modifier, a combination of an unlimited number of modifiers or no modifier.
  - **Key:** Key for the hotkey
  - **Autostart:** If this option is enabled, the Screenshot Tool function will be launched automatically when the thin client boots.
  - **Restart:** If this option is enabled, the Screenshot Tool function will be relaunched automatically after termination.
  - **Autostart Delay:** Waiting time in seconds between the thin client booting and the Screenshot Tool function being launched automatically.

### 7.13.1. Taking a screenshot

To take a screenshot, proceed as follows:

1. Launch the **Screenshot Tool** function. The launch options are described under *Screenshot* (page 106).
2. Select the area you would like to photograph. You have the following options:

- **Entire screen:** If this option is enabled, the entire screen contents will be photographed.
- **Active window:** If this option is enabled, the window which is currently the focus will be photographed.
- **Select a region:** If this option is enabled, you can freely select part of the screen using the mouse.
- **Capture the mouse pointer:** If this option is enabled, the mouse pointer will be visible on the screenshot.

3. Specify the **Delay before capturing** in seconds. The minimum value is 1.

4. Click on **Ok**.

If you have enabled **Entire screen** or **Active window**, the screenshot will be taken after the **Delay before capturing** has elapsed.

If you have enabled **Select a region**, you can select the desired part of the screen using the mouse. To do this, press and hold the left mouse button while dragging the mouse across the screen.

5. Specify how the screenshot is to be used. You have the following options:

- **Save:** If this option is enabled, the screenshot will be saved in PNG format via your thin client. You can save the screenshot locally, on a network drive or on a USB mass storage device.
- **Copy to the clipboard:** If this option is enabled, the screenshot will be available in the thin client's local cache. You can access the local cache from an RDP session and open the image in an RDP session application.
- **Open with:** If this option is enabled, the screenshot will be opened in your thin client's image viewer as soon as it is taken.

## 7.14. Soft keyboard

Menu path: **Setup > Accessories > Soft keyboard**

In this area, you can enable the **On-Screen Keyboard** for use with our IGEL UD10 or any other touchscreen.

In order to display the on-screen keyboard, you can either automatically launch it or show the **On-Screen Keyboard** button in the taskbar. These settings can be configured for the following cases:

- If the logon dialog is visible
- If the screen is locked



This setting has no effect on the on-screen keyboard in the **appliance mode**.

You can also influence which special keys are shown on the keyboard. These also apply for the **appliance mode**. The following three options are available to choose from:

- Function keys
- Navigation keys
- Numeric keys

➡ You will find additional settings under *Keyboard and Additional Keyboard* (page 134).

## 7.15. Java Manager

Menu path: **Setup > Accessories > Java Manager**

The Java Control Panel is an operating console which is used for various purposes.

- Specify how Java runs on your computer on the basis of various parameters.
- Manage temporary files used for the Java plug-in.

By doing this, you allow your web browser to use Sun Java to run applets and Java Web Start. As a result, you can launch Java applications via the network.

- Check certificates via the operating console. This gives you the security you need to use applets and applications via the network.
- Define runtime parameters for applets executed with Java plug-in and applications run with Java Web Start.

➡ Further information can be found at  
<http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>.

## 7.16. Monitor Calibration

Menu path: **Setup > Accessories > Monitor Calibration**

When calibrating your monitor (auto adjust), please use this special pattern. Generally speaking, you will achieve better results than if you calibrate the monitor with a conventional desktop and windows. Clicking on the pattern with the mouse closes the application again.

## 7.17. Commands

Menu path: **Setup > Accessories > Commands**

The following system commands can be made accessible to the user:

- Log out
- Sort symbols
- Switch off terminal
- Restart terminal
- Restart window manager

## 7.18. Network Diagnostics

Menu path: **Setup > Accessories > Network Tools**

The IGEL Universal Desktop Linux firmware features a number of tools for network analysis. These include:

- *Device information* (page 110)
- *Ping* (page 110)
- *Netstat* (page 111)
- *Traceroute* (page 111)
- *Look-up* (page 111)

### 7.18.1. Device Information

This tool provides information regarding the status of the network device used. This includes:

- MAC and IP address
- Link speed
- Various interface statistics (bytes transferred, errors etc.)

### 7.18.2. Ping

The **Ping** tool allows you to send contact queries to a network address. You can specify the exact number of queries to be sent. Alternatively, you can enable **Unlimited Requests** which means that the echo requests will be sent until you stop the process.

The Ping result is shown below, and the Ping duration of the last five Pings is illustrated in a bar chart.

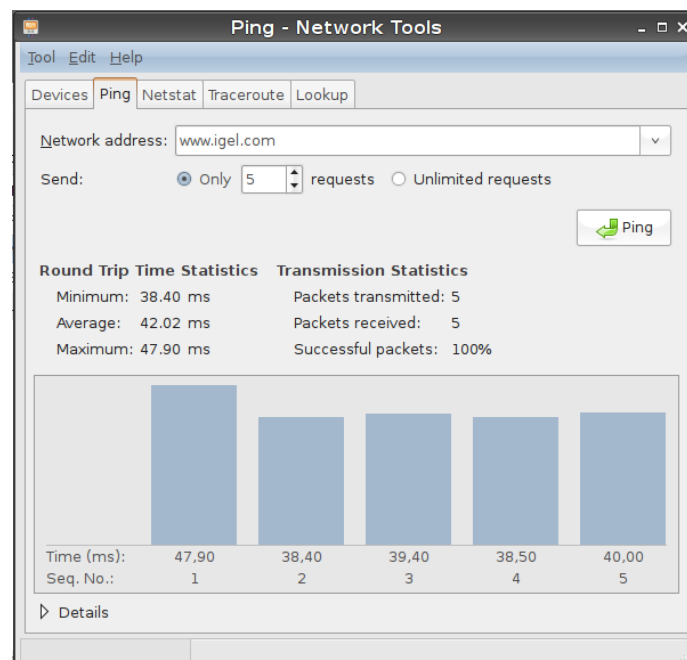


Figure 62: Ping network tools

- Enable **Program→Signal Tone for Ping** to configure the thin client to output an audible signal each time a Ping is sent.

### 7.18.3. Netstat

**Netstat** provides information on active network services with protocol and port information as well as a routing table and multicast information for your network devices.

### 7.18.4. Traceroute

With **Traceroute**, you can trace the route to a network address.

### 7.18.5. Look-up

The **Look-up** tool shows various information regarding your network address. The available information types are shown in this screenshot.

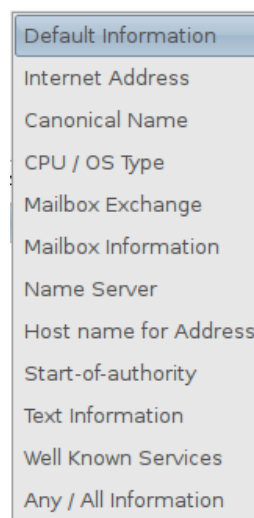


Figure 63: Information types for network address

## 7.19. System Information

Menu path: **Setup > Accessories > System Information**

The system information provides an overview of all internal and connected thin client hardware components as well as the constituent parts of the Linux system (e.g. kernel modules). The information shown can be copied to the clipboard in order to send it to the IGEL Support department for example.

## 7.20. Disk Utility

Menu path: **Setup > Accessories > Disk Utility**

Drive management shows all recognized USB drives along with their respective properties (device name, mount point etc.).

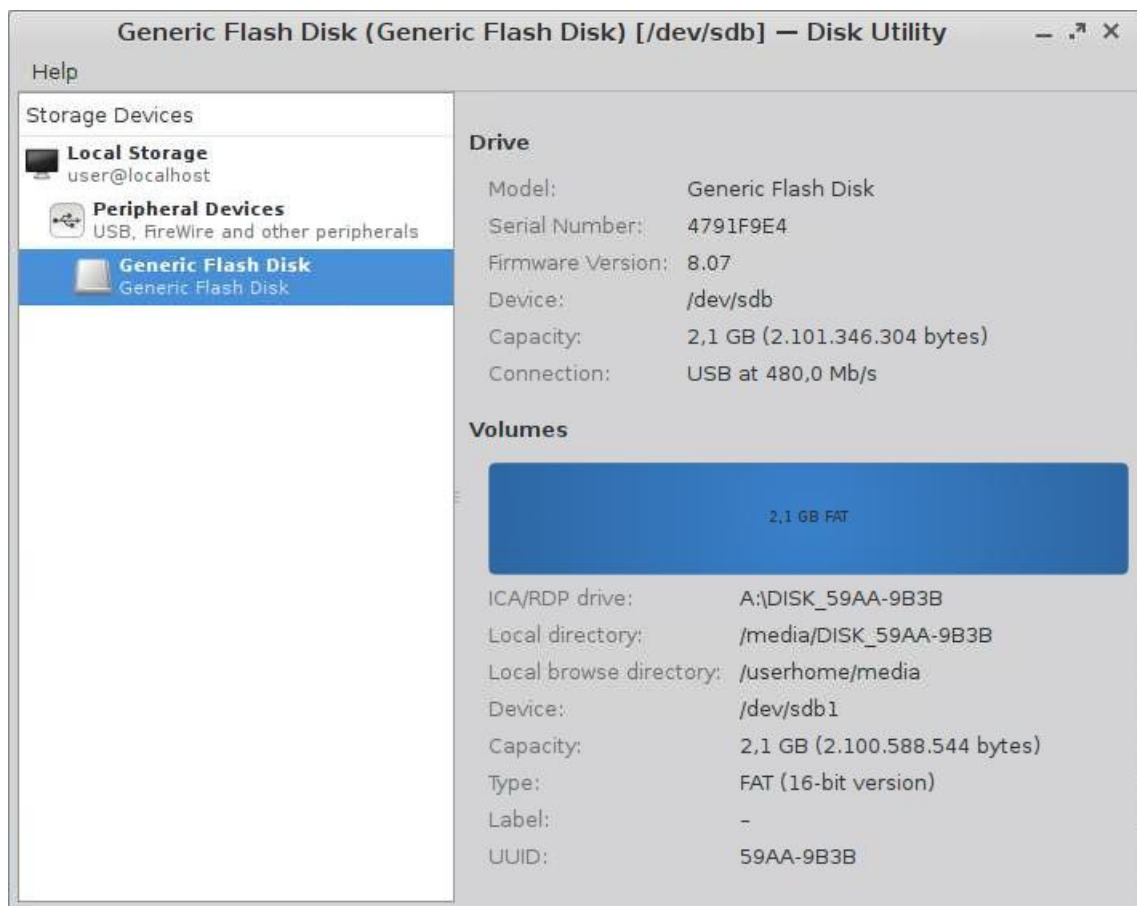


Figure 64: Drive management

- If Dynamic Client Drive Mapping is enabled, you will find a button to safely remove external drives here.
- You can configure a **Hotkey** for opening **Disk Utility**.

## 7.21. Firmware Update

Menu path: **Setup > Accessories > Firmware Update**

This session updates the firmware with the settings saved in **System > Update > Firmware Update**.

## 7.22. Smartcard Personalization

Menu path: **Setup > Accessories > Smartcard Personalization**

Configure the options to start the **Smartcard Personalization** (page 170).



## 7.23. Identify Monitors

Menu path: **Setup > Accessories > Identify Monitors**

Shows the screen number from the IGEL setup and hardware information on every connected screen.



Figure 65: Identify screens

## 7.24. Upgrade License

Menu path: **Setup > Accessories > Upgrade License**

You can distribute additional firmware functions via the IGEL Universal Management Suite or import licenses locally to a thin client. To do this, an IGEL USB stick with a smartcard or a storage medium containing licenses that have already been produced for this device must be inserted.



Figure 66: Firmware license upgrade

## 7.25. Webcam Information

Menu path: **Setup > Accessories > Webcam Information**

The **Webcam Information** tool reads information such as the manufacturer, model and supported video formats from a connected webcam. A test image from the camera with the chosen settings can also be displayed.

- Launch **Webcam Information** in the **Application Launcher (System)**.
- Select a resolution and click **Test** in order to display the camera image.

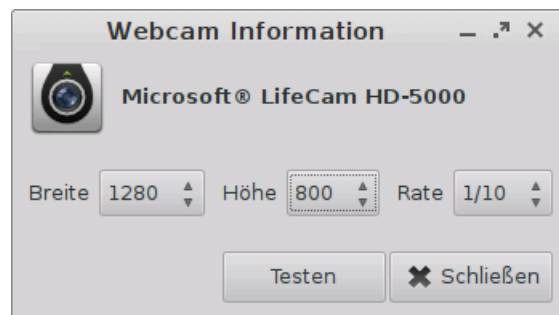


Figure 67: Webcam information



A list with all supported video formats can be created in the Linux Console using the command:  
`webcam-info -l`.

```

Local Terminal
root@IGEL-00E0C53627EE:/# webcam-info -l
Microsoft® LifeCam HD-5000
160x120:2/15
160x120:1/10
160x120:1/15
160x120:1/20
160x120:1/30
176x144:2/15
176x144:1/10
176x144:1/15

```

Figure 68: Command webcam-info -l

- ➡ In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open the website *cameroid.com* (<http://cameroid.com>) in your browser within the session (Adobe Flash must be installed).

## 7.26. Image viewer

The GPicview image viewer is installed from IGEL Universal Desktop Linux 5.06.100.



Applications such as the Firefox browser or the file manager use the image viewer as an auxiliary application. The image viewer does not have a menu entry for opening it directly.

The image viewer can be used to view a wide range of graphic MIME types:

- image/bmp
- image/gif
- image/jpeg
- image/jpg
- image/png
- image/x-bmp
- image/x-pcx
- image/x-tga
- image/x-portable-pixmap
- image/x-portable-bitmap
- image/x-targa
- image/x-portable-greymap
- application/pcx
- image/svg+xml
- image/svg+xml

➡ An entry in the FAQ (<https://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=680>) explains how you can change the way in which they are assigned.

➡ Instructions for using the image viewer can be found on *the Ubuntu Users website*. (<http://wiki.ubuntuusers.de/GPicview>)

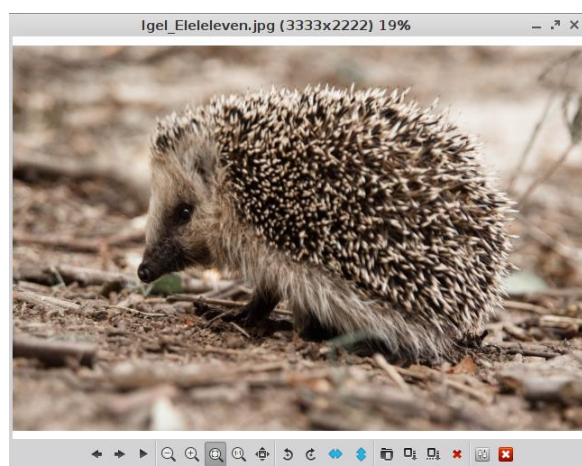


Figure 69: Image Viewer

## 8. User Interface

Configure the user interface exactly as you want it.

### 8.1. Screen

Menu path: **Setup > User Interface > Display**

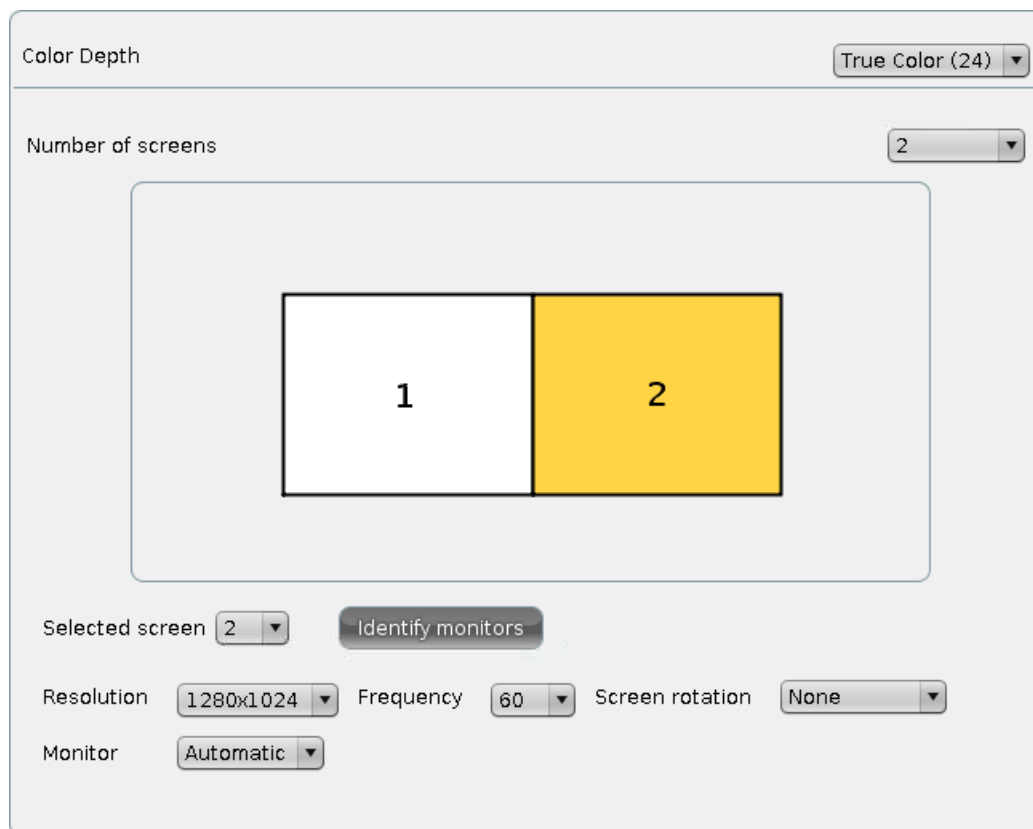




Figure 70: Screen settings

<b>Color Depth</b>	<p>Allows you to select the desktop color depth. The following options are available:</p> <ul style="list-style-type: none"> <li>16 bits per pixel (High Color / 65,000 colors)</li> <li>24 bits per pixel (True Color / 16.7 million colors)</li> </ul>
 Make sure that all screens connected to the thin client support the color setting.	
<b>DDC</b>	<p>Allows you to activate the Display Data Channel in order to share information between the system and the screen. If screen problems should occur, enable and disable the DDC setting in the <b>Options</b> by way of a test. DDC is enabled by default and the native resolution supported by the screen is determined automatically.</p>
<b>Screen configuration</b>	<p>Every screen connected to the IGEL UD device can be configured independently. The position of the individual screens can be determined in relation to Screen 1. Click on <b>Identify monitors</b> to show the screen identifier on each device.</p>

 For details of the display resolution supported by your IGEL thin client, please see its data sheet.

➔ If you use the Shared WorkPlace (SWP) feature with user-specific display resolutions, please note the *best practice on the subject* (<http://edocs.igel.com/index.htm#10202975.htm>).

### 8.1.1. Energy options

Menu path: **Setup > User Interface > Display > Power Options**

In this area, you can handle display power management. Your screen must support Display power management signaling (DPMS).

**Display power management settings**

☒ Handle display power management

	On battery	Plugged in
Standby Time	6 Minutes	10 Minutes
Suspend Time	8 Minutes	12 Minutes
Off Time	10 Minutes	15 Minutes

**Brightness reduction**

	On battery	Plugged in
On inactivity reduce to	20 %	80 %
Reduce after	Never	Never

Figure 71: Display power Management Options

- Enable **Handle display power management** in order to switch on the DPMS energy saving functions.
- Specify separately for battery and mains operation the number of minutes before the screen switches to a specific energy-saving mode:

Three different modes are offered:

- **Standby time** (standby mode)
- **Suspend time** (sleep mode)
- **Off time** (Off)

If a device is switched on but not used for some time, energy can also be saved by reducing the **brightness of the screen**.

- Specify by how many percent the brightness of the screen is to be reduced and how long the period of inactivity before brightness reduction should be. Values between 10 seconds and two minutes are available to choose from.



Naturally, all stages are gone through only if the X-Server does not receive any new entries during this period.

### 8.1.2. XDMCP

Menu path: **Setup > User Interface > Display > XDMCP**

Enable the XDMCP function for the screen in order to be able to select the appropriate connection type.



Please note that the local setup can then be accessed only using the hotkey **Ctrl+Alt+S**. This should therefore not be disabled for the setup application (**Accessories→Setup**).

Figure 72: Display XDMCP

<b>Connection type</b>	Allows you to select the appropriate connection type. If you select broadcast, the graphical logon from the first XDMCP server that responds to a broadcast query will be provided. If you choose the connection type indirect via local host, a list of XDMCP hosts will be shown during the startup procedure. Select from this list the host that provides the graphical logon.
<b>Name or IP of server</b>	This field is enabled if you select the connection type direct or indirect. Give the name or the IP address of the XDMCP server you wish to use. In the direct mode, you are provided with the graphical logon mask straight from the XDMCP server which you specified in the entry field. If you chose the indirect mode, a list of available XDMCP servers will be shown by the server you specified.



Make sure the Display Manager daemon (XDM, KMD, GDM ...) is running and that access authorization is available on the remote host.

### 8.1.3. Access control

Menu path: **Setup > User Interface > Display > Access Control**

Thin client **access control** is enabled by default. If you highlight **Switch off console access**, it will be possible to access your terminal screen from any UNIX host.

☐ Disable Console switching

---

☒ Access control

☒ Disable TCP connections

---

☐ Fixed X-Key

X-Key

---

List of Trusted X Hosts ★ 🗑️ 📄

Figure 73: Access Control

<b>Fixed X-Key</b>	You can grant specific users permanent remote access to your thin client. To do this, you will need to enable this option, click on the <b>Calculate</b> button and enter the 32-character key you have received into the Xauthority file on the user's computer.
<b>List of Trusted X hosts</b>	Click on the <b>Add</b> button to open the entry mask. Give the name of the remote host (not the IP address) you would like to add and confirm this by clicking on <b>OK</b> .

### 8.1.4. Gamma correction

Menu path: **Setup > User Interface > Display > Gamma correction**

In this area, you can increase or decrease the various brightness ranges in order to adjust the display on your screen to your preferences.

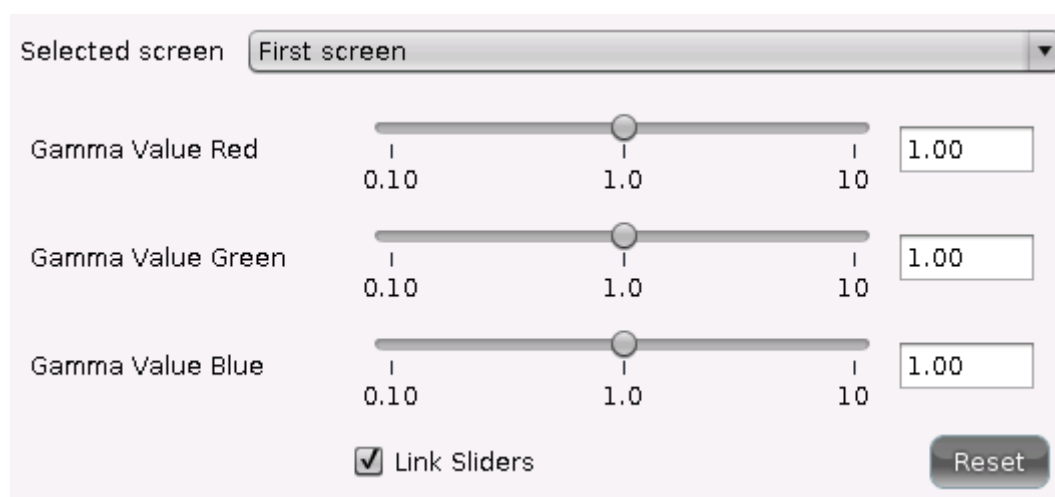


Figure 74: Gamma correction



### 8.1.5. Options

Menu path: **Setup > User Interface > Display> Options**

Configure the options for the display here:

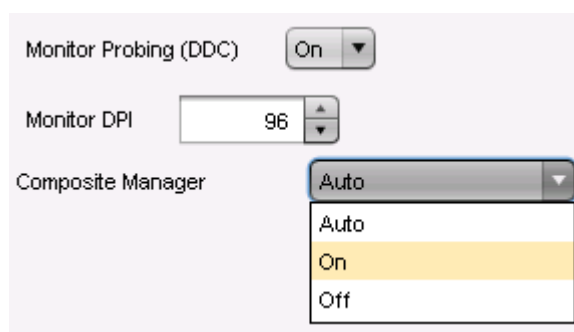


Figure 75: Display options

<b>Monitor Probing (DDC)</b>	Select <b>Off</b> in order to disable the automatic probing of display properties.
<b>Monitor DPI</b>	Enter the DPI resolution (dots per inch) for your monitor. The default setting is 96 DPI.
<b>Composite Manager</b>	<p>You will find three modes for the Composite Manager, the start menu and windows with animations and effects here:</p> <ul style="list-style-type: none"> <li>• Automatic: Disables the Composite Manager during battery operation, if the color depth is low or if the hardware is weak.</li> <li>• On</li> <li>• Off</li> </ul>

### 8.1.6. Universal MultiDisplay

The IGEL Universal MultiDisplay (UMD) solution enables you to set up an extended desktop with up to eight screens in any arrangement (the individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap).

A master thin client (master) can be connected to up to three satellite thin clients (satellite), while one or two screens can be connected to each of the thin clients within the group. Only the master is connected to the company network. The satellites are connected, via their own network, only to the master, which must have a second network card for this purpose.

All other peripherals such as a keyboard, mouse etc. are connected to the master. The entire system is also configured on the master, either via its local setup or the IGEL Universal Management Suite UMS.

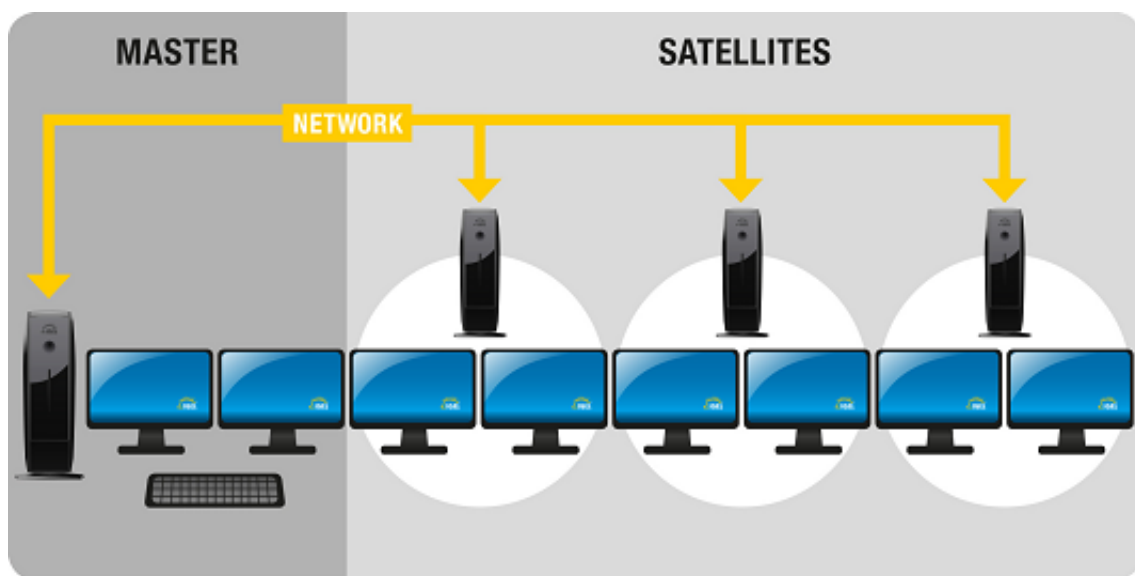


Figure 76: IGEL Universal MultiDisplay Setup

### Software Requirements

The following software requirements must be met in order to use IGEL Universal MultiDisplay:

- IGEL UD Linux firmware offering IGEL Universal MultiDisplay support on the master and satellites



Note: Devices with IGEL Universal Desktop OS cannot be used for IGEL Universal MultiDisplay.

- IGEL Universal MultiDisplay Starter Kit license for up to three displays (2x master, 1x satellite)
- IGEL Universal MultiDisplay license for each additional display connected



Note: You will receive the Starter Kit license along with the master thin client. Licenses for additional displays can be added to the master thin client in the IGEL Universal Management Suite Console (**System > License Management**).

## Hardware and Network Requirements

The following requirements must be met in order to use IGEL UMD:

- Master: IGEL UD5-x30 LX thin client with PCIe network card installed
- Satellite: Up to 3 IGEL thin clients with Universal Desktop Linux
- The master is connected to the company network via the internal Ethernet port. The additional PCIe network card is used to connect one satellite directly, or a number of satellites via an intermediate switch.
- Depending on the particular hardware configuration, screens can be connected to the master and the satellites via the VGA, DVI or display port.

## Advanced Options

In the IGEL Registry under **Setup→System→Registry**, you will find a number of additional parameters which are not yet available in the actual screen configuration:

**x.dmx.number\_of\_screens\_master** and **x.dmx.number\_of\_screens\_slaveX** allow you to define only one connected monitor for a particular thin client (the default setting is two available monitors per device). This makes sense if two or more UD5s, each with a high-resolution monitor, are to be connected together via the display port for example.

The master saves the list of available satellites. A satellite can be deleted from the list via the **x.dmx.slaveX** parameter by selecting Delete Instance.

The satellites can be arranged in any order by making changes in **x.dmx.slaveX.number**. However, there is no consistency check, so you must therefore carry out a manual check to ensure that the numbering is clear.

With **x.dmx.net**, the automatic configuration of the internal network between the master and clients can also be carried out manually, e.g. the IP address of the master or the address area of its DHCP server.

## Configuration

Once you have connected the master and satellites to each other as described above, switch on the master thin client. In the master setup, enable IGEL Universal MultiDisplay under **User Interface→Screen→IGEL Universal MultiDisplay**.

Select the number of screens and set the resolution, rotation etc. for each one. You can select the screens from the list or simply by clicking on them in the arrangement overview.

Using drag & drop, arrange the screens in the overview in the same way as they are physically arranged. When all screens are configured, confirm your choices by clicking on **OK**.

Now switch on the satellites, one after another, starting with satellite 1. After powering up a satellite, wait around 30 seconds before switching on the next one. The satellites will receive their configuration, including IP address, from the master. IGEL Universal MultiDisplay is now ready for use.

## Usage

Once you have carried out the initial setup procedure as described above, you will not need to touch the satellites again. The satellites are automatically shut down when you switch off the master and reactivated when the master boots. Subsequent firmware updates will also be distributed automatically to the satellites by the master. All changes to the screens' configuration (arrangement and resolution of the screens, desktop background for each screen, screensaver etc.) should be made on the master (locally or via the UMS). Naturally, this also applies to all other options, e.g. sessions.

You can move application windows freely over all the screens and enlarge the windows so that they cover screen boundaries. If you maximize windows, they are usually enlarged to cover the area of the current screen. Depending on the session type, sessions in full-screen format may be restricted to a specific screen or can be expanded across all screens.

## 8.2. Desktop

Menu path: **Setup > User Interface > Desktop**

With the help of the following five dialog fields, you can configure the appearance and behavior of the desktop, windows, task bar, pagers (virtual screens) and start menu.

On this page, you can configure general settings for the appearance of the desktop:

- Change the **user interface themes**,
- Specify **fonts**
- Change the **desktop icon size**
- Configure the display and delay time for **tool tips**.

<input checked="" type="checkbox"/> Local Window Manager for this Display	
Tooltip Delay Time	<input type="text" value="500"/>
Tooltip Display Time	<input type="text" value="600"/>
Userinterface Theme	<input type="text" value="IGEL-light"/>
Desktop Icon Size	<input type="text" value="64"/>
<b>Desktop Fonts</b>	
Default Font	<input type="text" value="Sans"/>
Default Font Size	<input type="text" value="10"/>
Desktop Icon Font Size	<input type="text" value="11"/>
Titlebar Font	<input type="text" value="Sans Bold"/>
Titlebar Font Size	<input type="text" value="11"/>

Figure 77: Desktop

### 8.2.1. Background

Menu path: **Setup > User Interface > Desktop > Background**

In this area, you can configure the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient.

You can also use a background of your own.



You can set up a separate background image for each monitor connected to the thin client.



Wallpaper (1st Monitor)	<input type="text" value="Igel blue (4x3)"/>
Wallpaper Style (1st Monitor)	<input type="text" value="Stretched"/>
Color Style (1st Monitor)	<input type="text" value="Solid Color"/>
Desktop Color (1st Monitor)	<input type="button" value="Choose color"/> 
2nd Desktop Color (1st Monitor)	<input type="button" value="Choose color"/> 
<input checked="" type="checkbox"/> Enable Custom Wallpaper Download (1st Monitor)	
Custom Wallpaper file (1st Monitor)	<input type="text"/>

Figure 78: Wallpaper

## Custom wallpaper - server configuration

Wallpaper	Here, you can set up the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient. You can also use a background image of your own. You can set up a separate background image for each monitor that is connected to the thin client.
Custom Wallpaper Download	<p>A user-specific background image can be provided on a download server. In the <b>Desktop→Background</b> window, enable the option <b>Enable Custom Wallpaper Download</b> and give the name of the background image file. You can specify the download server in the <b>Desktop→Background→Custom Wallpaper</b> window. If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.</p> <p>The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually (Update Background Image). The download can also be launched from the IGEL Universal Management Suite via <b>Update desktop changes</b>.</p>



The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an **custom wallpaper** and **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

➡ For further instructions on how to customize your IGEL Linux desktop see our best practice.

### 8.2.2. Taskbar

Menu path: **Setup > User Interface > Desktop > Taskbar**

In this area, you can enable and configure the taskbar.

You can change the following settings:

- **Use taskbar:** If this option is enabled, the taskbar will be displayed.
- **Taskbar Position:** Specifies the position in which the taskbar is displayed.

Possible values:

- **Bottom**
- **Top**
- **Left**
- **Right**

- **Vertical Taskbar Mode:** Specifies how items are shown in the taskbar. This parameter is available if **Taskbar Position** is set to **Left** or **Right**.

Possible values:

- **Vertical:** The session texts are rotated by 90°.
- **Deskbar:** The session texts are not shown.
- **Taskbar Height/Width:** Specifies the height of the taskbar in pixels.



If **Number of rows/columns in Taskbar** is set to **Automatic**, the window buttons as well as the symbols in the Quick Start Panel will be shown in a number of rows depending on the height of the taskbar. The number of rows increases in increments of 55 pixels:

- 1 - 55 pixels: One row
- 56 - 110 pixels: Two rows
- 111 - 165 pixels: Three rows
- 166 - 220 pixels: Four rows
- 221 - 275 pixels: Five rows
- 276 or more pixels: Six rows

The **Maximum number of rows/columns in window button list** parameter is described under *Taskbar Items* (page 128).

- **Number of rows/columns in taskbar:** Specifies the number of rows for the Quick Start Panel. The following taskbar items can be broken down into a number of rows and columns: Symbols in the Quick Start Panel, window buttons,
  - **Automatic:** The number of rows for the Quick Start Panel depends on the height and width of the taskbar.
  - **Numeric value:** The chosen value specifies the number of rows for the Quick Start Panel.
- **Dualview Taskbar Size:** Specifies whether the taskbar is expanded across a number of monitors or restricted to one monitor.
- **Monitor:** Specifies the screen on which the taskbar is shown. This parameter is available if **Taskbar size in dual view** is set to **Restrict taskbar to one monitor**.
- **Taskbar on top of all windows:** If this option is enabled, the taskbar is always shown, even in sessions with a full-screen window.
- **Taskbar Auto Hide:** If this option is enabled, the taskbar is hidden and will only be shown if the mouse pointer is moved to the position of the taskbar at the edge of the screen.
- **Auto Hide Behavior:** Specifies when the taskbar is automatically hidden.

Possible values:

- **Intelligently:** The taskbar is shown as standard. The taskbar will be hidden if the space is needed by a window, e. g. a window in full-screen mode.
- **Always:** The taskbar is hidden as standard. The taskbar will be shown if the mouse pointer is moved to the edge of the screen.
- **Taskbar Show Delay:** Time interval in milliseconds before the taskbar is shown. The mouse pointer must be at the edge of the screen constantly during this time interval. This setting is only effective if **Taskbar Auto Hide** is enabled.



With the show delay, you can prevent the taskbar for a full-screen session being covered by the thin client's taskbar. A show delay is necessary if the taskbar for the full-screen session is set to be shown automatically and both taskbars are positioned at the same screen edge. If no show delay is set and the user brings up the taskbar for the full-screen session, this will immediately be covered by the thin client's taskbar.

During the show delay time interval, the user has time to move the mouse pointer away from the edge of the screen.

- **Taskbar Hide delay:** Time interval in milliseconds before the taskbar is hidden. This setting is only effective if **Taskbar Auto Hide** is enabled.

➡ Further settings can be found under *Screen Lock/Saver* (page 131).

### 8.2.3. Taskbar background

Menu path: **Setup > User Interface > Desktop > Taskbar Background**

You can specify the background style for the taskbar here.

To incorporate your company logo into the taskbar, proceed as follows:

1. Select **Background Image** under **Background Style**.
2. Give the path of the background image.

➡ See also *Taskbar* (page 126) under User Interface.

### 8.2.4. Taskbar items

Menu path: **Setup > User Interface > Desktop > Taskbar Items**

- **Taskbar Clock:** If this option is enabled, a clock will be shown in the taskbar.
- **Sorting order in window button list:** Specifies the criteria according to which the window buttons are sorted.

Possible values:



- **Timestamp:** The window buttons are sorted in the chronological order in which the windows were opened.
- **Group and time stamp:** The window buttons are grouped according to the type of application. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted chronologically.
- **Window title:** The window buttons are sorted alphabetically.
- **Group and window title:** The window buttons are grouped according to type. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted alphabetically.
- **Drag'n'Drop:** You can order the buttons as you wish using drag and drop. You must drag a button over at least half of the button to be skipped.
- **Maximum number of rows/columns in window button list:** Specifies the maximum number of rows available for window buttons.

Possible values:

- **Automatic:** The number of rows depends on the **Taskbar height/width** and **Number of rows/columns in taskbar** parameters, see *Taskbar* (page 126).
- **Numeric values:** This value specifies the maximum number of rows.
- **Show labels in window button list:** If this option is enabled, the names of ongoing sessions are shown in the associated window buttons. If this option is disabled, only the symbols are shown.
- **Taskbar System Tray:** If this option is enabled, the system tray will be shown in the taskbar.
- **Size of icons in system tray:** Specifies the size of system tray icons (volume, network connection etc.).

You can choose a pre-defined value or enter a numeric value between 1 and 64.

Predefined values:

- **Automatic:** The size is adjusted to the height and width of the taskbar.
- **Small:** 20 pixels
- **Medium:** 40 pixels
- **Large:** 60 pixels

➡ Further settings can be found under *On-screen Keyboard* (page 108), *Keyboard and Additional Keyboard layouts* (page 134) and *Screen Lock/Saver* (page 131).

### 8.2.5. Pager

Menu path: **Setup > User Interface > Desktop > Pager**

In this area, you can enable the use of a number of virtual workstations.

The **Pager** is a tool with virtual desktops which can be used as an easy way of switching between open applications. This window is shown at the right of the task bar. You can use up to 25 virtual desktops. If you use a **Pager**, you can switch between full-screen applications for example at the click of a mouse.

Instead of minimizing/maximizing sessions or switching between them using key combinations, you simply click on the desired screen using the mouse. The screen is then shown as it was when you closed it (unless you restarted the system beforehand).

Figure 79: Desktop Pager

### 8.2.6. Start menu

Menu path: **Setup > User Interface > Desktop > Start Menu**

In this area, you can configure the desktop start menu:

Figure 80: Desktop Start menu

There are three start menu types:

<b>Legacy:</b>	Standard setting which is similar to that from Windows 95 - a list of available sessions and options
<b>Advanced:</b>	An expanded start menu featuring a search function and a more attractive design It requires more resources, which is particularly noticeable on slow devices.
<b>Auto:</b>	Automatically select the classic or advanced start menu depending on the processor.

## 8.3. Language

Menu path: **Setup > User Interface > Language**

Select the system language from the list. You can also set the keyboard layout and the input language depending on the system language.



The language selected is the language for the user interface and therefore applies to all local applications.

## 8.4. Screen Saver and Screen Lock

Menu path: **Setup > User Interface > Screen Lock/Saver**

You can set up the screen saver so that it is activated either automatically or in response to a key combination (**hotkey**). You can also select a password option. The look of the taskbar can be configured separately for the login dialog and the locked screen.

Example configuration of a screen lock:

### General

The screen can be locked via taskbar or desktop icons or using hotkey **Ctrl-Shift-L**.

Figure 81: Startup Options of Screen Lock

## Options

The screen lock starts automatically after 5 minutes without user action at the thin client. The screen lock can be stopped by entering a user password or administrator password (see *Password* (page 169)).

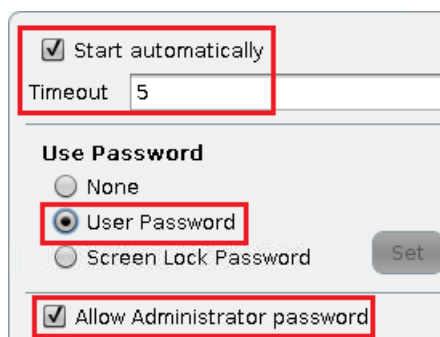


Figure 82: Autostart and Password Settings

## Taskbar

The locked screen does not display the taskbar until the login dialog appears. The user can bring up a soft keyboard, e.g. to login using touchscreen monitor.

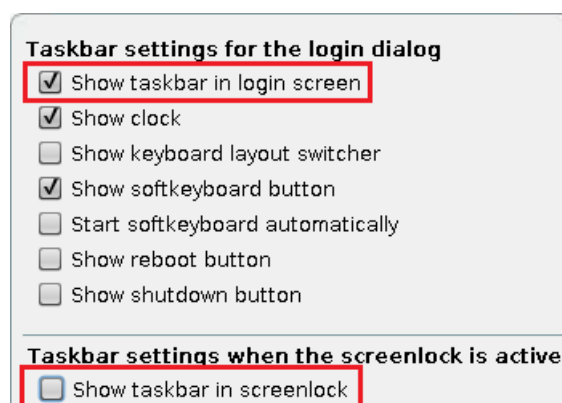


Figure 83: Taskbar on Login Dialog

### 8.4.1. Example configuration for the screen saver

Menu path: **Setup > User Interface > Screen Lock/Saver > Screensaver**

The session for the **screen saver** can show both a custom image and a configurable clock.

You can select the color of the background, display a custom image (or several images as a slide show) or a digital clock whose size and color can be changed. A combination of a company logo and the clock can also be displayed.

➡ In our best practice you will find an example configuration and further instructions on how to customize your IGEL Linux desktop.

1. Connect a network drive with your saved images.



You can also send images to the thin client, e.g. to a /wfs/pix target directory, using UMS file transfer.

2. Enable the displaying of images in the configuration menu for the screen saver and use the network drive connected beforehand as the source.

Screen background color Choose color

---

☒ Enable image display

Image file/directory

☒ One image per monitor

Image duration

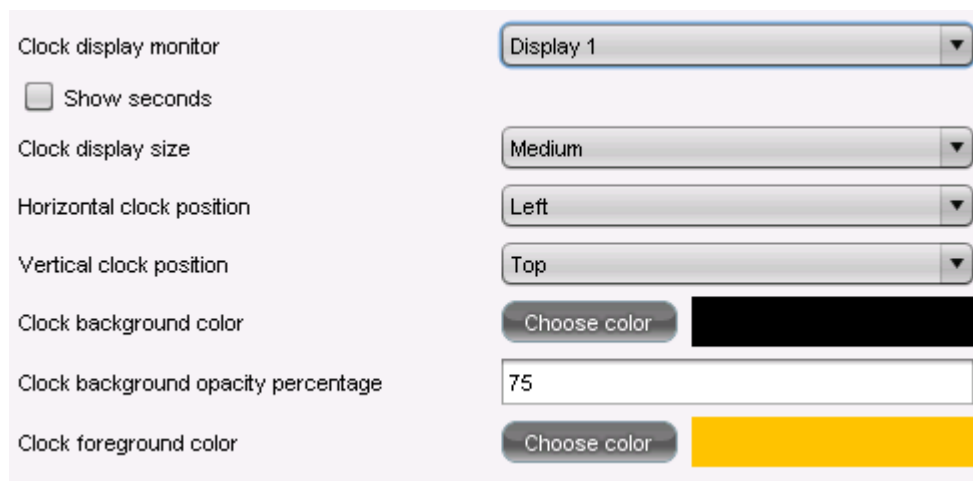
Image display mode Small-sized hopping ▼

Figure 84: Select image source



If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.

- You can configure a digital clock (size, position on the screen and colors) independently of the screen display. The seconds display can be disabled.



Clock display monitor: Display 1

☐ Show seconds

Clock display size: Medium

Horizontal clock position: Left

Vertical clock position: Top

Clock background color: Choose color [Black swatch]

Clock background opacity percentage: 75

Clock foreground color: Choose color [Yellow swatch]

Figure 85: Clock configuration

## 8.5. Input

Menu path: **Setup > User Interface > Input**

These setup pages allow you to set the keyboard layout and other input options.

The following input devices can be configured:

- *Keyboard* (page 134)
- *Mouse* (page 135)
- *Touchscreen* (page 138)
- *Signaturpad* (page 139)

### 8.5.1. Keyboard and additional keyboard

Menu path: **Setup > User Interface > Input > Keyboard**

In this area, you can configure the keyboard.

- **Keyboard layout** – Determines the keyboard layout. The selected layout applies for all parts of the system including emulations, window sessions and X applications.
- **Keyboard type** – Determines the keyboard type.
- **Key repeat** – Determines the automatic repeat behavior for the keyboard:
  - **Repeat delay** – Determines the delay (in milliseconds) before automatic repetition begins.
  - **Repeat rate** – Determines how often a character repeats per second.
  - **Enable dead keys** – Enable this function if the keyboard used supports dead keys for special characters.
- **Start with NumLock on** – Stipulates that **NumLock** is to be automatically enabled during the boot procedure.

Menu path: **Setup > User Interface > Input > Additional Keyboard Layouts**

- You can define **additional keyboard layouts** which can be selected by the user. The layout can be selected in the taskbar or changed via configurable hotkeys.
- ➡ Further settings can be configured under *On-screen Keyboard* (page 108).

### 8.5.2. Mouse

Menu path: **Setup > User Interface > Input > Mouse**

<b>Mouse type and mouse connection</b>	Determines the type of mouse used and how it is connected
<b>Left-handed mode</b>	Changes the orientation of the mouse by switching the mouse buttons to left-handed mode.
<b>3-button mouse emulation (no support for serial mouse)</b>	Enables/disables emulation of the third (middle) mouse button for mice with only two physical buttons. This third button is emulated by pressing both buttons at the same time. If 3-button emulation was enabled, the emulation time limit determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.
<b>Mouse speed</b>	Determines the mouse resolution in counts per inch
<b>Mouse double-click interval</b>	Changes the maximum interval (in milliseconds) between two consecutive mouse clicks which are to be recognized as a double-click.

### 8.5.3. Touchpad

Menu path: **Setup > User Interface > Input > Touchpad**

If you use the Universal Desktop Converter, you have the option of defining touchpad settings.



The actual options depend on the particular touchpad.

You will find these under **User Interface > Input > Touchpad**.

The settings options are subdivided into

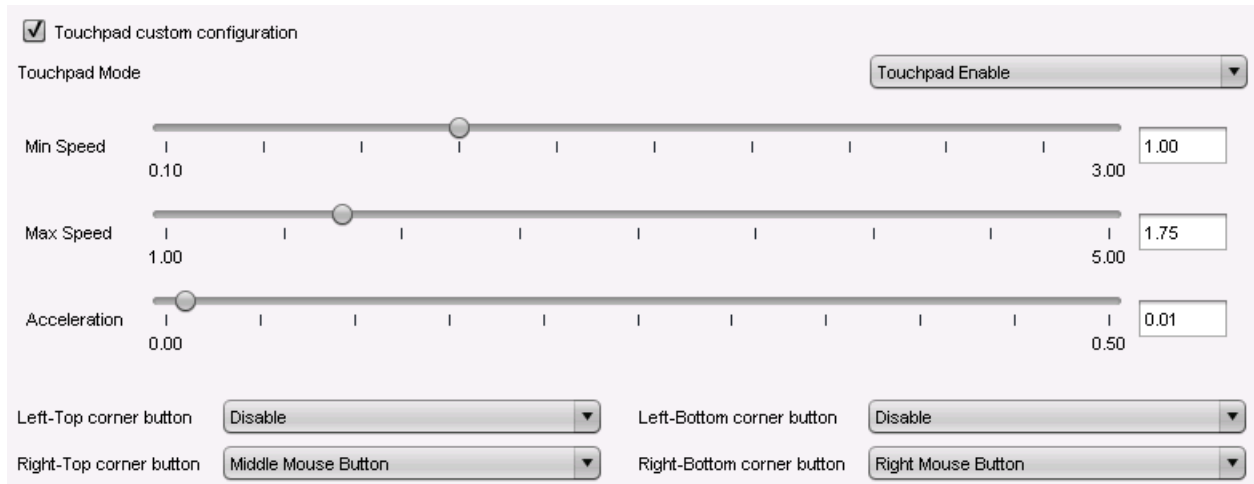
- *Touchpad General* (page 135)
- *Touchpad Scrolling* (page 136)
- *Touchpad Advanced* (page 137)

## Touchpad General

Menu path: **Setup > User Interface > Input > Touchpad**

In this area, you can configure the touchpad according to your needs.

- Enable **Touchpad custom configuration** in order to define personal settings.



☒ Touchpad custom configuration

Touchpad Mode: Touchpad Enable

Min Speed: 0.10 | 1.00 | 3.00

Max Speed: 1.00 | 1.75 | 5.00

Acceleration: 0.00 | 0.01 | 0.50

Left-Top corner button: Disable

Left-Bottom corner button: Disable

Right-Top corner button: Middle Mouse Button

Right-Bottom corner button: Right Mouse Button

Figure 86: General settings for the touchpad

- Select a touchpad mode from:
  - **Enable touchpad** - Decide whether you would like to enable the touchpad by default...
  - **Disable touchpad** - ... or disable it.
  - **Disable tapping and scrolling** - As an alternative, you can disable tapping and scrolling only.
- Use the sliders to set the speed of the mouse pointer in seconds.
- With a number of touchpads, you can assign functions to the four corners. The following settings apply by default:
  - **Left mouse button** - Tap on the relevant corner to highlight objects, place the cursor and move text or objects from one place to another.
  - **Middle mouse button** - Tap on the relevant corner to bring up program-specific functions.
  - **Right mouse button** - Tap on the relevant corner to display the context menu.
  - **Disable** - Tap on the relevant corner to disable the mouse button.



## Touchpad scrolling

Menu path: **Setup > User Interface > Input > Touchpad**

Define the properties for vertical and horizontal scrolling here.

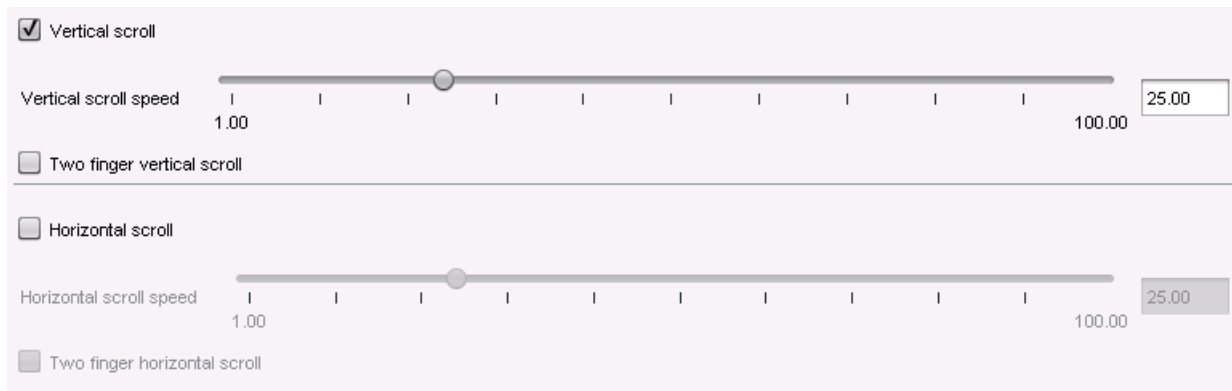


Figure 87: Scrolling properties for the touchpad

- Enable **Vertical scrolling** in order to set the **vertical scroll speed**.
- Enable **Horizontal scrolling** in order to set the **horizontal scroll speed**.

## Touchpad Advanced

Menu path: **Setup > User Interface > Input > Touchpad**

Further settings are possible here:

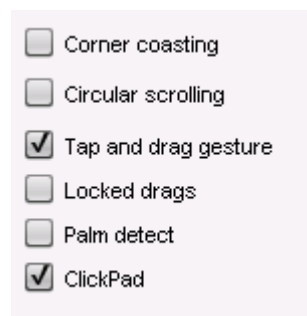


Figure 88: Advanced settings for touchpad

- Enable the following functions in order to...

<b>Corner coasting</b>	continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges.
<b>Circular scrolling</b>	scroll in a circular fashion. In the selection menu, specify where circular scrolling is to begin.
<b>Tap and drag gesture</b>	move items by tapping and dragging them.
<b>Locked drags</b>	end the tap and drag gesture only after an additional tap; it will otherwise end when you let go.
<b>Palm detection</b>	avoid triggering a function accidentally with the palm of your hand. The function must be supported by the device.
<b>ClickPad</b>	allow ClickPads. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.

## Touchscreen

Menu path: **Setup > User Interface > Input > Touchscreen**

To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected. The setup procedure with an on-screen keyboard is described below.

### Touchscreen drivers

The touchscreen types currently supported are:

- Elographics serial touchscreens
- TSharc serial touchscreens
- EvTouch USB touchscreens

➡ You will find the complete list of supported devices in the IGEL Linux 3rd Party Hardware Database.

- **Touchscreen already calibrated**

If you enable the touchscreen function, the touchscreen must be calibrated first. Unless you enable this option, calibration will begin automatically after each system boot.

- **Swap X and Y values**

Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction.

- **Minimum/maximum X value/Y value**

These values are determined by the calibration tool. However, you can also change them manually.

- **Let-go limit**

The maximum permitted time (in milliseconds) between two instances of contact in order to still be registered a single touch. When moving windows by drag-and-drop, for example, your contact with the screen may inadvertently be interrupted. Increasing this value prevents the thin client from registering two individual contacts in this case.

- **Contact limit**

Determines how long (in milliseconds) the screen needs to be touched in order for the contact to be recognized.

- **Baud rate (for serial touchscreens only)**

Determines the speed of communication via the selected connection. (If in doubt, read the monitor manual.)

- **Touchscreen connection**

You can connect the touchscreen either to COM1 or COM2. Select your preferred connection here.

- **Set driver-specific default settings**

Click on this button once after changing the touchscreen type or to restore the default settings.



A list of the touchscreens currently supported by IGEL Linux can be found in the IGEL Linux 3rd Party Hardware Database.



Enable the on-screen keyboard for touchscreen use in the setup under **Accessories > On-screen Keyboard**.



The layout for the normal keyboard will also be used for the on-screen keyboard.



Calibrate the touchscreen for optimum contact recognition. The touchscreen calibration application can be found under **Application Launcher > System**.

After launching the calibration program, you will see a pattern with calibration points which must be touched one after another.

#### 8.5.4. SCIM (Input Methods)

Menu path: **Setup > User Interface > Input > SCIM Input Methods Platform**

**Smart Common Input Method (SCIM)** platform offers entry methods for over 30 languages under Linux. You can enable one of the methods provided by the IGEL system for Chinese character sets (Simplified Chinese, Traditional Chinese) or manage generic tables for describing the entry method.

#### 8.5.5. Signature pad

Menu path: **Setup > User Interface > Entry > Signature Pad**

The following signature pads are available for connection to IGEL Linux thin clients:

- Softpro
- StepOver TCP
- signotec VCOM Daemon



Enable the **Softpro SPVC signature pad channel** in the IGEL Setup under **Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**.

To enable the **StepOver TCP Client** in order to be able to use USB signature pads from this manufacturer in sessions, proceed as follows:

1. Select the checkbox for **StepOver TCP Client**.

If necessary, you can change the TCP port.

2. Click on **Apply**.

➡ You will find detailed information regarding the configuration of signature pads in the Best Practice documents for StepOver Pads and Softpro/Kofax pads.

To enable the **signotec VCOM Daemon** in order to be able to use USB signature pads from this manufacturer in sessions, proceed as follows:

1. Select the checkbox for **signotec VCOM Daemon**.
2. Click on **Apply**.
3. Go to **Mapping > Serial Connections** under ICA or RDP Global.
4. Enable **COM Port Mapping**.
5. Click on **Add** and choose one of these devices **Search Devices**.

Under **Select Available Device**, you can choose from the signotec devices `/dev/ttyVST0` and `/dev/ttyVST1`.

6. Select one of these devices.
7. Your signotec signature pad can now be used.

## 8.6. Hotkeys

Menu path: **Setup > User Interface > Hotkeys > Commands**

In order to make it easier to use your thin client, hotkeys are available for frequent operating routines. A hotkey is a combination of one or more modifiers and an alphanumeric key.

You can enable or disable hotkeys and change the keys used.

To enable or disable a hotkey, proceed as follows:

1. Highlight the hotkey in the list.
2. Click on **Modify...**
3. Enable or disable the **Hotkey** option in the dialog window.
4. Click on **Continue** in the dialog window.
5. Click on **Apply** or **OK**.

To change the keys used for a hotkey, proceed as follows:

1. Highlight the hotkey in the list.
2. Click on **Modify...**
3. In the **Modifiers** selection list, select a modifier, no modifier or a combination of modifiers.
4. Enter the **Key**.
5. Click on **OK** or **Cancel**.

The following hotkeys are available and can be changed:

- Hide all windows and show desktop
- Screenshot of active window
- Screenshot of entire screen
- Volume up (multimedia key)
- Volume down (multimedia key)
- Volume mute (multimedia key)
- Switch between active windows using Task Switcher
- Switch between active windows using Task Switcher (backwards)
- Switch focus to next window
- Switch focus to next window (2)
- Enable next window (reverse order)
- Open start menu
- Open start menu (2)

## 8.7. Font Services

Menu path: **Setup > User Interface > Fonts Services**

You can import further fonts in addition to those provided by IGEL:

- *XC font service* (page 141)
- *NFS font service* (page 141)

### 8.7.1. XC Font Service

Menu path: **Setup > User Interface > Fonts Services > XC Font Service**

If you need other fonts in addition to those offered by the thin client, you can use the XC font service.



This service must be installed on a server and fully configured there.

The advantage of using the XC font service rather than NFS is its better performance.

➤ Click on **Enable XC Font Service** in order to enable the following entry fields.

<b>XC font server</b>	Give the name of the server on which the XC font service operates.
<b>Port number</b>	Give the number of the port used by the font service for reception purposes - the default setting is port number 710.
<b>Favor local fonts</b>	Enable this option if local fonts are to be used before a request is sent to the font server.

### 8.7.2. NFS Font Service

Menu path: **Setup > User Interface > Fonts Services > NFS Font Service**

Using the **NFS font service** is another way to import additional fonts. The NFS font service also offers the advantage that the mount point for the fonts can be configured. This is necessary for a number of remote applications that search for your fonts in a specific directory.

- Define and enable an NFS font path entry in order to use the NFS font service.

This will be added to the **list of NFS mounted font directories**.

- Click on **Add** to open the dialog window:

<b>Local directory</b>	Defines the local directory for the mount point
<b>NFS server</b>	Name or IP address of the server that makes available the font directories via NFS.
<b>Server path</b>	Path on the server under which the fonts are available.
<b>Favor local fonts</b>	If this option is enabled, local fonts are to be used before a request is sent to the font server.

- Click on **Enable** to enable the entry.
- Export the font directory to the server via NFS read-only for the thin client.

## 9. Network

Menu path: **Setup > Network**

Configure the thin client's network connections here.

### 9.1. LAN interfaces

Menu path: **Setup > Network > LAN Interfaces**

- Click on **Network > LAN interfaces** in the client setup.
- Choose between automatic network setup with the protocols DHCP and BOOTP or manual network configuration in order to set the thin client for each network interface.

☒ Activate default interface (Ethernet)

☒ Get IP from DHCP Server  
☐ Specify an IP Address

IP Address

Network Mask

Default Gateway ☐ enable

Terminal Name

☐ Enable DNS

Default Domain

Nameserver

Nameserver

☐ Manually overwrite DHCP settings  
☐ Dynamic DNS Registration

Dynamic DNS Registration Method

TSIG key file for additional DNS authentication

Figure 89: LAN Interfaces

DHCP	Via the Dynamic Host Configuration Protocol, the thin client receives its IP address, network mask, DNS, gateway and other network configurations from a DHCP server. DHCP is enabled by default for LAN 1 (internal). DHCP options can be enabled in the <b>DHCP Client</b> menu. A list of standard options is available. However, you can also define your own options.
BOOTP	Via the <b>BOOTP</b> , the thin client receives its IP address, network mask, DNS, gateway and other network configurations from a BOOTP server database.



The transferring of a `setup.ini` file or a boot script is not supported. BOOTP is not used to call up a boot image from a server and boot this image, in spite of what the term may imply.

Specify IP address manually	Configures the network settings manually instead of searching for a DHCP server. Ensure that the fixed IP address that you enter is not used by another computer in your network. If you have to use a gateway to forward the data packages to and from the target network, click on <b>Enable</b> and enter the gateway IP address.
Terminal name	Give the local name of the thin client. Otherwise, the standard name IGEL <MAC address> will be generated.
Enable DNS	Configures the DNS - Specify the <b>standard domain</b> in which the device will work as well as the IP address of up to two <b>name servers</b> which will be queried one after the other.
Manual overwrite DHCP settings	Manual entries overwrite the standard route, the domain name and the DNS servers.
Dynamic DNS registration	Here, you can automatically report the current IP address of the thin client to the DNS. The <b>DHCP</b> and <b>DNS</b> methods are available. If you select <b>DNS</b> , you may have to specify a <b>private TSIG key for DNS authentication</b> .

➡ You can find instructions for dynamic DNS registration via DNS in an FAQ document.

### 9.1.1. Individual interface

Menu path: **Setup > Network > LAN Interfaces > [Interface]**

Under the name of the individual interface (for example Interface 1), you can overwrite some of the general settings for LAN interfaces. In addition, there are two further settings:



IPv6 configuration	Here, you can choose a configuration type for operation with IPv6. You will find further details in a best practice document.
Network link type	Specify the network link type for the interface. The default is <b>Automatic Recognition</b> .

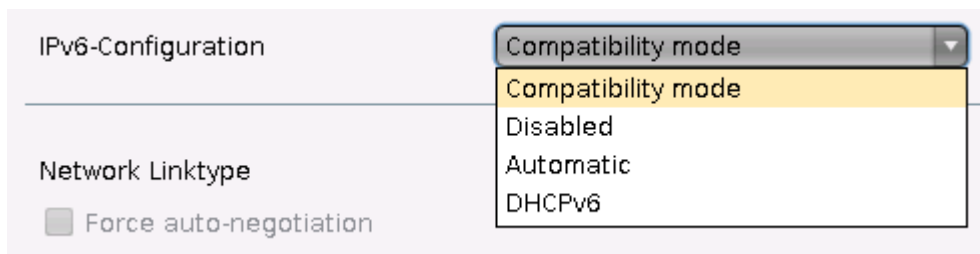


Figure 90: Configuration of an individual interface

## Authentication

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Authentication**

You can enable and configure network port authentication in accordance with the IEEE 802.1x standard here. The following settings are available:

- **Enable IEEE-802.1x authentication:** This option enables network port authentication.
- **EAP Type:** You can choose between the **PEAP** and **TLS** authentication procedures here.



For the **EAP Type** PEAP, the following phase 2 authentication methods are available to choose from under **Auth Method**:

- **MSCHAPV2**
- **TLS**
- **GTC**
- **MD5**

- **Validate Server Certificate:** If this option is enabled, the certificate of the server will be checked cryptographically. In order to do this, the path to the CA certificate file is required in **CA Root Certificate**. The file can be in PEM or DER format.



A number of the following fields need to be filled in only for specific combinations of **EAP type** and **Auth Method**.

- **Manage certificates with SCEP (NDES):** Automatically manage client certificates with **SCEP** (page 156)
- **Identity:** The user name for network access
- **Password:** The password for network access



If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

- **Client Certificate:** Path to the file with the certificate for client authentication in the PEM (base64) or DER format. If a private key in the PKCS12 format is used, leave this field empty.
- **Private key:** Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER or PFX format. The **Private Key Password** may be required for access.

## Wake-on-LAN

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Wake on LAN**

Select the packages or messages with which the thin client can be started via the network.

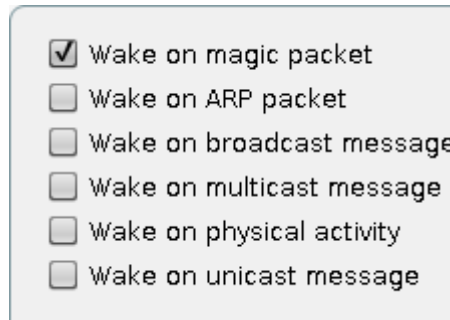


Figure 91: Wake-on-LAN options

### 9.1.2. Wireless

Menu path: **Setup > Network > LAN Interfaces > Wireless**

In this area, you can configure everything relating to your WiFi connections.

➡ You will find details of compatible WiFi modules in our IGEL Linux 3rd Party Hardware Database.

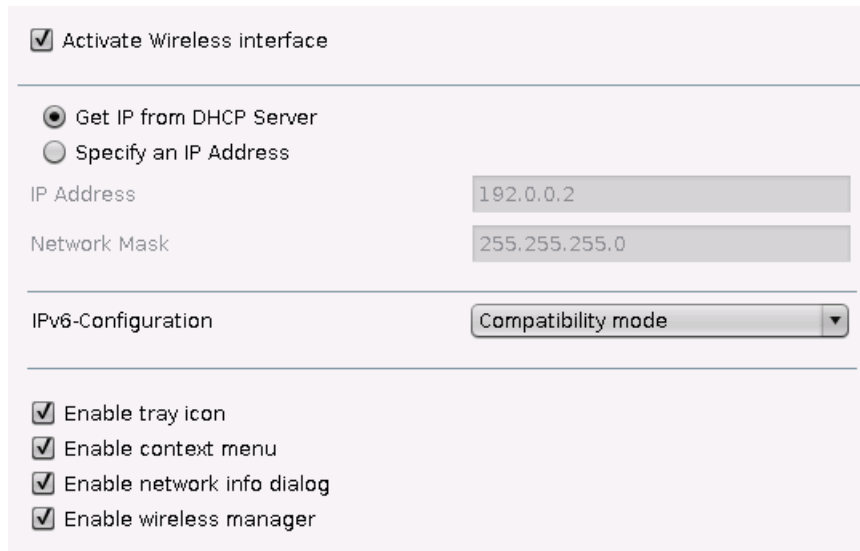
If you use mobile devices and regularly spend time in different WIFI zones, you will benefit from our new function: IGEL Café Wireless. This means that you can

- easily connect to new, previously unknown WIFI networks
- save connections that you have set up and then reuse them later on

straight from the user interface via the **Wireless Manager** as you would with a smartphone. This function is irrelevant for stationary desktop devices that are managed centrally. In this case, it is assumed that the network has fixed settings and cannot be influenced by the end user.

To configure the WIFI interface, proceed as follows:

1. Open the **IGEL Setup** and click on **Network→LAN Interfaces→Wireless**.



The screenshot shows the 'Wireless' configuration window in IGEL Setup. At the top, there is a checkbox labeled 'Activate Wireless interface' which is checked. Below this, there are two radio buttons: 'Get IP from DHCP Server' (selected) and 'Specify an IP Address'. Under the 'Specify an IP Address' option, there are input fields for 'IP Address' (containing '192.0.0.2') and 'Network Mask' (containing '255.255.255.0'). Below these fields is a dropdown menu for 'IPv6-Configuration' set to 'Compatibility mode'. At the bottom, there are four checked checkboxes: 'Enable tray icon', 'Enable context menu', 'Enable network info dialog', and 'Enable wireless manager'.

Figure 92: Enable user-defined connections

2. Enable the **Wireless Interface**.
3. Select the configuration for your **IP-Addresses** (DHCP or manual).
4. Select a configuration type for operation with **IPv6**.
5. Enable at least the **Tray Icon**, **Context Menu** und **Wireless Manager**. Via the **Wireless Manager** you can use IGEL Café Wireless.



Ensure that the **Overwrite Sessions** parameter is disabled for UMS profiles with this Wireless configuration. Otherwise, user-defined connections will be lost when the thin client is rebooted.

6. Configure the wireless network connection in the **Default WiFi network** (page 151), if you do not select it via the .

Additional connections can be configured in the **Additional WiFi networks** (page 151)

7. Configure your location in the **WiFi frequency range** (page 152).

Once these settings become active on the thin client, a new symbol for wireless connections will appear in the system tray:



Figure 93: WiFi symbol

## Wireless Manager

You can bring up the **Wireless Manager** from the tray icon:

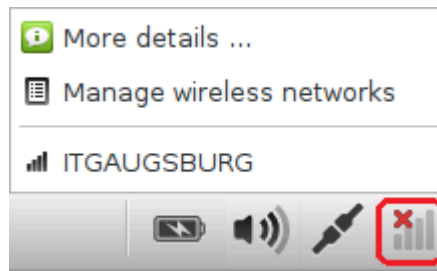


Figure 94: Symbol bar with WiFi context menu



You will need to have switched on the **Wireless Manager** under **Network→LAN Interface→Wireless**.

1. Click on the **Wireless** tray icon in the taskbar and then on **Manage wireless networks** in order to bring up **Wireless Manager**:

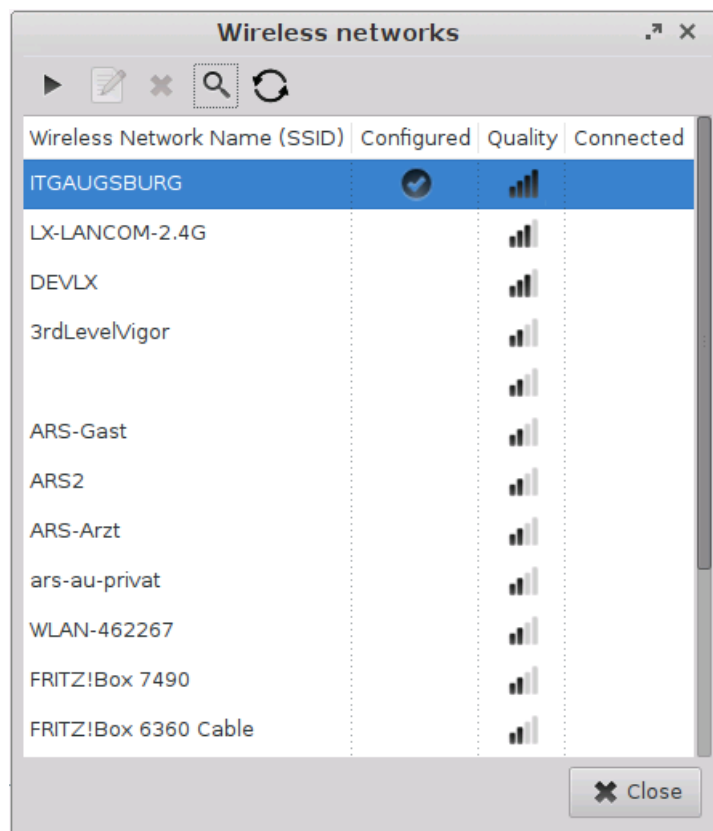


Figure 95: Wireless Manager

2. Search for available networks.

- The list of active networks is sorted according to the quality of their signal strength.
  - Previously configured connections are flagged with a tick in the **Configured** column.
  - The connection currently active is likewise flagged with a symbol under **Connected**.
3. Double click on a network in the list in order to open the entry mask. If you are using the **Wireless Manager** for configuration, you only need to give the network key – this is considerably easier than using the Setup or the UMS for configuration:



Figure 96: Configure WiFi connection

You can either **permanently store** the logon information or enter it each time you establish a connection to this network.



Click on the key symbol in order to display the key phrase while you are typing.

1. Click on the **Connect Network** button in order to establish the previously configured connection:

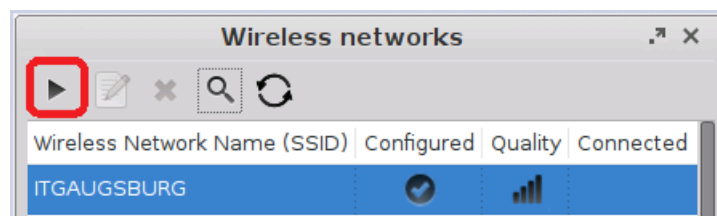


Figure 97: Establish connection to WiFi

The tray icon will change and show the quality of the connection to the active network.

Hidden networks appear in the **Wireless Manager** with the network name empty or can be defined using the **Search for Network** button:

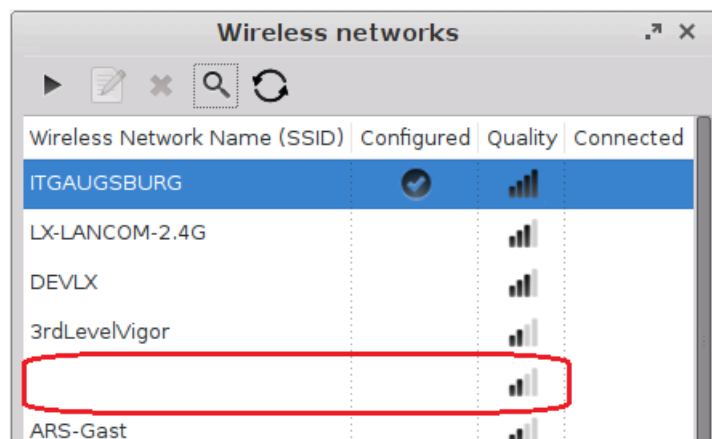


Figure 98: Hidden network

In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

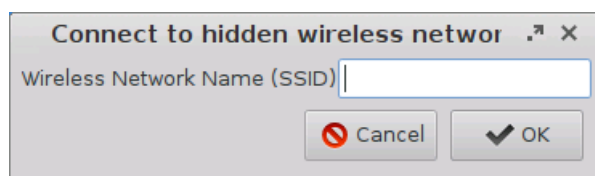


Figure 99: Name of the hidden network



If you have configured the available connections, you will no longer need the **WiFi Manager** in order to establish a connection.

In the context menu for the tray icon, all available networks are listed and can be brought up from here.

- The IGEL Setup shows all connections configured by the local user locally and in the UMS under **Network→LAN Network→Wireless→Additional WiFi networks**:

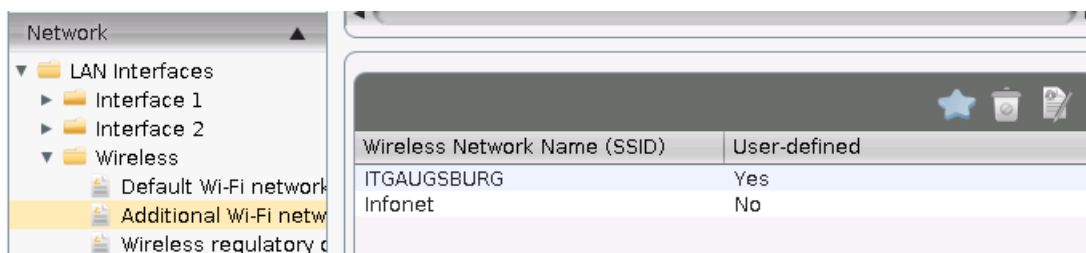


Figure 100: User-defined WiFi connections in the IGEL Setup



A **Yes** in the **User-defined** column means that you can change or delete this connection in the **WiFi Manager**. A connection that you have set up in the **WiFi Manager** is automatically user defined. Connections that are specified in the Setup or in the UMS can also be flagged as user defined. In most cases, however, this would not make much sense. After all, the end user should only be able to delete the connections that they themselves have set up, e.g. when traveling.

## Configure connections in the setup

Menu path: **Setup > Network > LAN Interfaces > Wireless > Default Wi-Fi network /Additional Wi-Fi networks**

In the **Default WiFi network** and **Additional WiFi networks** areas, you can configure wireless network connections:

Figure 101: WiFi configuration

1. Select an **Encryption** method.
2. Enter the **Network Name (SSID)**.
3. Set further parameters depending on the encryption method selected.



For WPA(2) Enterprise encryption, the client certificate can also be requested and administered via SCEP. See *Network/SCEP* (page 157) and our Certificate Enrollment and Renewal with SCEP (NDES) best practice.

The connections defined under **Additional WiFi networks** have the same value as the connection entered under **Default WiFi network**. Here, you can pre-configure WiFi connections which are available for selection by the user in the *Wireless Manager* (page 148).

The connections configured in the **Wireless Manager** are likewise shown in the **Additional WiFi networks** list and are automatically flagged as **User-defined**.

## Connections to hidden networks

Hidden wireless networks (WIFI without SSID broadcasting) can also be connected to. Pre-defined connections can be used without disclosing the network name to the user. For user-defined connections, the user must however know the name of the hidden network.

To pre-configure connections to hidden networks, proceed as follows:

- In the **IGEL Setup**, go to **Network→LAN interface→Wireless→Default WiFi network** and set the **AP-Scan mode** parameter to **No broadcast**.

Enable WPA Encryption

Network key: \*\*\*\*\* ☐ show

AP Scan mode: no broadcast

Figure 102: Connection configuration for hidden networks

Additional connections can be configured in the **Additional WiFi networks** dialog.

## Wireless regulatory domain

Menu path: **Setup > Network > LAN Interfaces > Wireless > Wireless regulatory domain**

In this area, you can configure your location:

Wireless regulatory domain: Europe

Location: United Kingdom

Channel No.	Center frequency (GHz)	Channel flags
-------------	------------------------	---------------

Figure 103: WiFi frequency ranges



Ensure that the WiFi frequency range is configured correctly in order to prevent your device making illegal transmissions.

### 9.1.3. DHCP Options

Menu path: **Setup > Network > DHCP Client > Standard Options / Custom Options**

Configure the client's use of DHCP options - a number of **standard options** are already set out in a list and can be enabled. **User-defined options** can be set up in a list of your own and managed there.



### 9.1.4. Virtual Private Network - VPN

Menu path: **Setup > Network > VPN**

Remote users securely access company networks via virtual private network protocols (VPN). You can set up your client accordingly for this purpose.

#### PPTP

Menu path: **Setup > Network > VPN > PPTP**

PPTP (point-to-point tunneling protocol) is one of the most common virtual private network (VPN) protocols allowing remote users to securely access company networks.

##### Automatically establishing a connection during the boot procedure

In order to set up a client which is fully configured to automatically establish a connection, you may need to dial up first.

1. Enable this option before the desktop is launched.  
The client connects to the host.
2. Click on **Add** to set up new connections.
3. Configure the necessary settings in order to dial up the RAS server on the desired remote station.
4. Select the network device and specify whether a dial-up connection is to be used.
5. Specify on the **Options** tab the name service and the IP configuration for the PPTP connection.



These data will normally be transferred from the remote station's RAS server. This means that both DNS and IP address will be set to **automatic** by default.

You can set up additional network routes on the next three setup pages (Routing).

#### OpenVPN

Menu path: **Setup > Network > VPN > OpenVPN**

The OpenVPN client puts in place a virtual private network using TLS encryption and requires OpenVPN 2.x as a VPN server.

It supports the following authentication methods:

- TLS certificates
  - Name/password
  - Name/password and certificates
  - Static key
- Click on the star symbol to set up a new OpenVPN connection.
- ➡ A best practice document describes setting up OpenVPN connections.

## NCP

Menu path: **Setup > Network > VPN > NCP**

The configuration parameters for the NCP Client are configured exclusively via the client program interface itself.

➡ You will find the documentation regarding the NCP Secure Enterprise Client at:  
<http://www.ncp-e.com/de/support/produktunterlagen/handbuecher.html>

## GeNUCard

Menu path: **Setup > Network > VPN > GeNUCard**

The dedicated VPN device GeNUCard offers preconfigured Internet and VPN connections.

After starting a GeNUCard session the connection dialog opens. Various start options can be configured under **Desktop integration**.

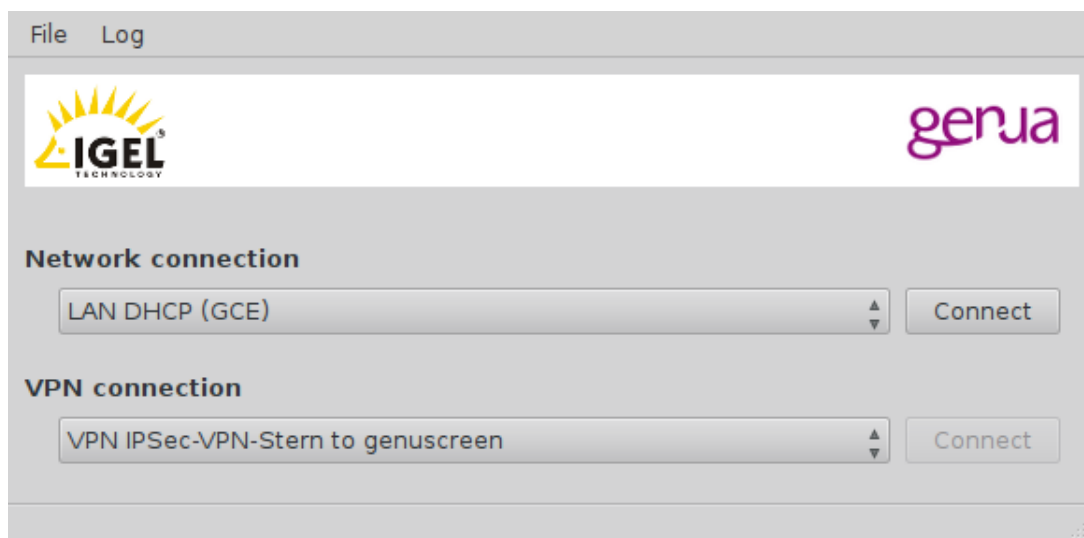


Figure 104: GeNUCard configuration

The **File** menu lists entries to **Change PIN** and for **Rekeying**.

## GeNUCard Options

Menu path: **Setup > Network > VPN > GeNUCard > Options**

A valid combination of connection and user data can be entered in Setup under **Network > VPN > GeNUCard > Options**.

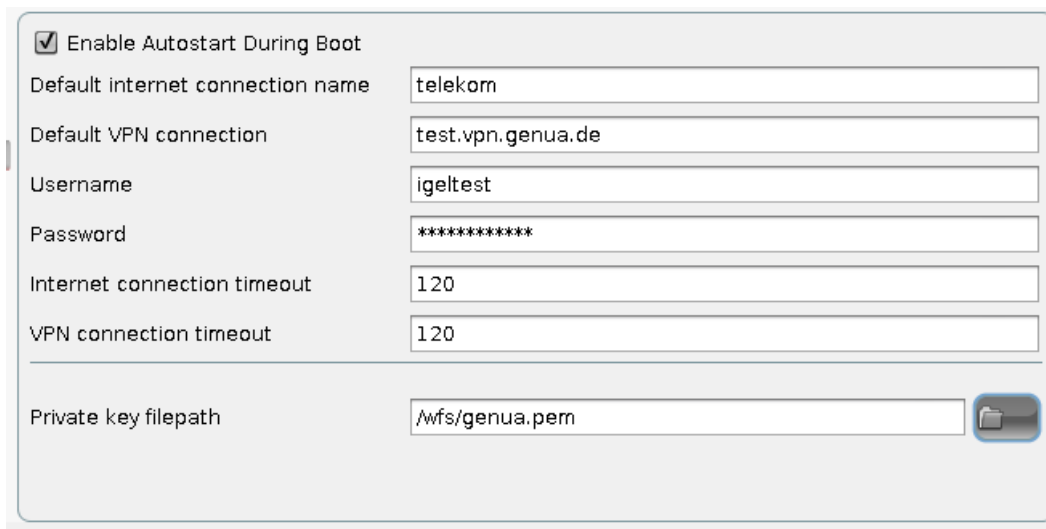


Figure 105: Automatically establishing connections

There is also an option for autostarting the connection during boot, which is required for updating the IGEL firmware over VPN.

## GeNUCard Administrator Session

➡ Use the genucenter software to configure and manage your GeNUCard. For further information refer to [www.genua.de](http://www.genua.de).

Optionally you can set up an administrator session for configuring the Internet connection for GeNUCard:

1. Click **Add Instance** under **System > Registry > genucard%**.

A GeNUCard icon appears on the Desktop.

2. Click the GeNUCard icon.

The GeNUCard login window opens.

3. Enter **Username** and **Password**.

4. Click **OK**.

The Internet/VPN window opens..

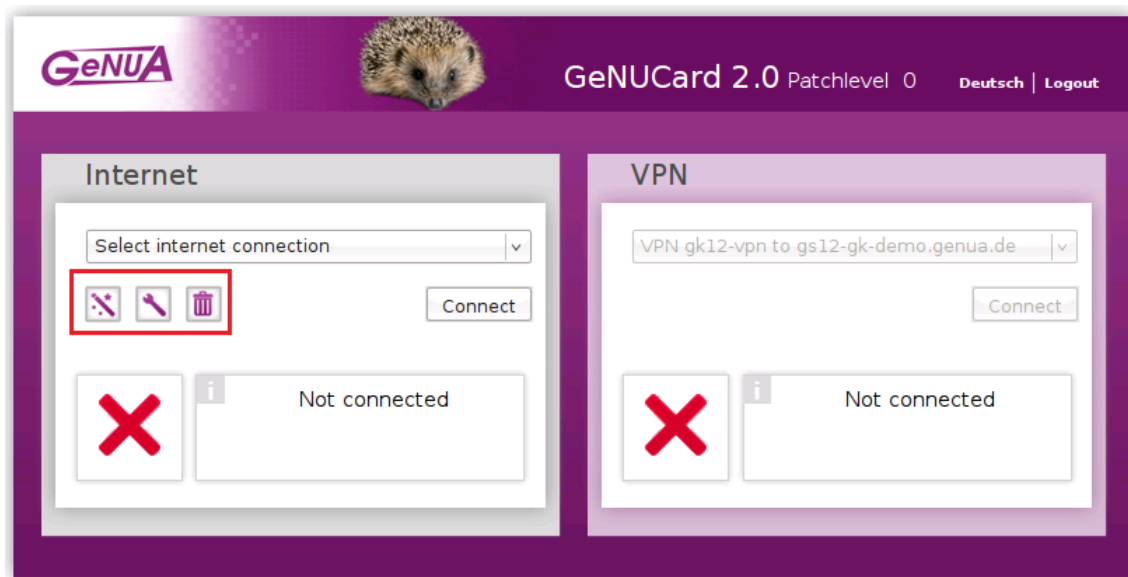


Figure 106: Internet/VPN window

5. Under **Internet** use the **New**, **Modify** and **Delete** buttons to configure the Internet connection.

### 9.1.5. Simple Certificate Enrollment Protocol - SCEP

Menu path: **Setup > Network > SCEP Client (NDES)**

SCEP allows the automatic provision of client certificates via a SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x).

A Microsoft Windows 2008 Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification authority).

- ➡ More information can be found at Microsoft, e.g. in the white paper <http://download.microsoft.com/download/a/d/f/adf2dba9-92db-4765-bf2d-34b1c8df9ca3/Microsoft%20SCEP%20implementation%20whitepaper.doc>
- Enable certificate management via SCEP client (NDES) and then make the necessary configuration settings.

### Certificate

Menu path: **Setup > Network > SCEP Client (NDES) > Certificate**

- Under **Certificate**, specify the basic date for the certificate to be issued by the certification authority.

Type of CommonName	If the client automatically obtains its network name, DNS Name (auto) is a good type of thin client certificate.
Organizational unit	Stipulated by the certification authority.
Organization	A freely definable designation for the organization to which the client belongs.
City, state, country	Enter the location of the client here.
RSA key length	Select a key length (one able to be used by the certification authority) for the certificate that is to be issued.

## Certification Authority

Menu path: **Setup > Network > SCEP Client (NDES) > Certification Authority**

- Enter the name of the certification authority (CA) and the hash value of the root certificate.

You will receive both of these from the certification authority.

## SCEP

Menu path: **Setup > Network > SCEP Client (NDES) > SCEP**

In addition to a certification authority, an SCEP server must also be defined.

- Enter the **address** and **query password** for the SCEP server here.



The SCEP server generates the password as a one-time password. It is needed when a certificate is requested for the first time. New certificates will be requested before the old ones expire. In this case, the still-valid certificate will serve as a means of authentication.

- For the purpose of checking validity, define an **interval** (checking frequency) and a **period of time** in which certificate renewal must occur.

Example:



A certificate is valid until 31.12 in any one year. The period for renewal is 10 days. This means that a new certificate will first be requested on 21.12 of the same year.



Because of the need to enter a fingerprint (root certificate of the certification authority) and the query password (SCEP server), the configuration process is somewhat awkward. Ideally, it should be set up in the UMS as a profile and distributed to the clients. At the same time, the certificate still cannot be used for communication purposes.

## Checking the Client Certificate

If a certificate from the certification authority has been forwarded from the SCEP server to the client, it is then stored there in the `/wfs/scep_certificates` folder.

The data for the certificate (e.g. its validity, creation date and hash value) can be displayed by using the shell command `cert_show_status`.

## Example

Certificates issued and managed via SCEP can be used for purposes such as network authentication.

Relevant options can be found when

- configuring IEEE 802.1x authentication

**Network→LAN Interfaces→Interface 1→Authentication**

- or when setting up the wireless network

**Network→LAN Interfaces→Wireless→Authentication, WPA Enterprise Encryption, EAP Type TLS.**

One problem when the client certificate is distributed via the network is that the same certificate is needed for communication. The use of the SCEP in conjunction with 802.1x authentication presents no problems to the extent that the initial request for the certificate should also be possible without a certificate.

➤ Enable the 802.1x authentication method after the SCEP has been configured.

When requesting the certificate, the client will attempt to establish a connection to the SCEP server without using any authentication. It will use the authentication only after having received the certificate.

For WLAN connections, a method of certificate-less PSK encryption must first be set up. The client will then use this connection to obtain the certificate. After this, the WLAN connection can be reconfigured once again.

While the above-mentioned method for Ethernet connections will also function via the UMS, the initial configuration of the WLAN can only be performed on the client as the WLAN is disabled by default.

### 9.1.6. Routing

Menu path: **Setup > Network > Routing**

This setup page allows you to specify additional network routes if necessary.

➤ In the **Interface** field, specify "eth0", "eth1" or "wlan0", i.e. Interface 1+2 or Wireless LAN.

You can specify up to five additional network routes.

### 9.1.7. Hosts

Menu path: **Setup > Network > Hosts**

If no DNS (Domain Name Service) is used, you can specify a list with hosts in order to allow translation between your IP address, the full qualified host name and the short host name.

Click on **Add** to open the dialog window.

1. Enter the **IP address** of the host you would like to add.
2. Give the **full qualified host name** (e.g. <mailserver.igel.de>).
3. Give the **short host name** of the host (e.g. <mailserver>).
4. Confirm the details you have entered by clicking on **OK**.

The specified host will now be added to the computer list.

### 9.1.8. Network Drives

Menu path: **Setup > Network > Network Drives**

Drives shared within the network can be linked to the thin client via NFS or SMB - depending on the protocol offered by the server.

#### NFS

Menu path: **Setup > Network > Network Drives > NFS**

With NFS (Network File System), you can share files via the network. The NFS server exports a system file, and the NFS client (your thin client) links this file to a mount point within its own file system. The exported file system then becomes a logical part of the thin client file system although, in physical terms, it remains on the server.

➡ In order to set up an NFS mount, the server must first be configured. You will find detailed information on NFS on the relevant pages of the manual for your server operating system.

The procedure for sharing files via the NFS server is as follows:

➤ Click on **Add** to open the dialog window for NFS.

You can then enter the following:

Enabled	The NFS mount is enabled by default and is mounted each time the system boots. Disable this entry if the shared file system is not universally needed.
Local directory	Details of the local directory onto which the shared items are to be mounted on the local thin client file system.
Server	The name or IP address of the NFS server which provides the shared files.
Path name	Details of the path name as exported by the NFS server.

#### Windows Drive - SMB

Menu path: **Setup > Network > Network Drives > Windows Drive**

SMB is used by Microsoft Windows NT, Windows 95/98, Windows 2000 and Windows XP etc. to share hard drives and printers. As Unix (including Linux) can process this protocol with Samba Suite tools, hard drives and printers can be used along with Windows hosts. Consequently, items shared via SMB can be integrated into the thin client by Windows or Unix Samba hosts.



The SMB protocol is used only to share files via the network (not for printers). Shared items which are to be mounted must first be created on the Windows or Unix host.

Local directory	Details of the local directory onto which the shared items are to be mounted on the local thin client file system.
Server	For a Windows host, the Net BIOS name must be entered here. For a Unix Samba host, the host name or the IP address must be used.
Share path name	Path name as exported by the Windows or Unix Samba host.
User name/password	Details of the user name and password for your user account on the Windows or Unix Samba host.
Enabled	The SMB mount is enabled by default and is mounted each time the system boots.
Writable for users	If this option is enabled, the user who is logged on can write data. Otherwise, this is only possible via root.

## 9.2. Proxy

Menu path: **Setup > Network > Proxy**

Select the communication protocols for which a system-wide proxy is to be used.

☐ Direct Connection to the internet  
☒ Manual proxy configuration

FTP Proxy:   
 HTTP Proxy:   
 SSL Proxy:   
 SOCKS Host:   
 SOCKS Protocol version: SOCKS v5  
 No Proxy for:

Figure 107: System-wide proxy



# 10. Devices

Menu path: **Setup > Devices > Hardware info**

- Click on **Hardware Information** for an overview of your IGEL thin client device.

## 10.1. Printers

Menu path: **Setup > Devices > Printer**

Various printing systems can be used with the thin client.

### 10.1.1. CUPS - Common UNIX Printing System

Menu path: **Setup > Devices > Printer > CUPS**

The Common UNIX Printing System™ (CUPS) is the software which allows you to print from within applications, e.g. from this web browser.

CUPS converts the page descriptions produced by the application, e.g. "Insert Paragraph", "Draw Line" etc., into data which can be read by the printer, and then sends this information to the printer.

With the appropriate configuration, CUPS can use printing devices via the following connections:

- Parallel (LPT 1, LPT 2)
- Serial (COM1, COM2, USB COM1, USB COM2 – with USB serial adapter)
- USB (1st and 2nd USB printer)
- Network (TCP/IP, LPD, IPP)

### Printers

Printers can be created and edited here.

- In the edit dialog, specify a printer name which begins with a letter.

### General

- Under **Printer Connection**, select the interface type for locally connected printers or the network protocol for network printers.
- Enter the relevant configuration data for the interface or network printer.
- Select the local printer driver under **Manufacturer and Printer Name**.

## Mapping in sessions

Map printer in NX sessions:	Makes the printer available in NX sessions.
Map printer in ICA sessions:	Makes the printer available in ICA sessions.
Map printer in RDP sessions:	Makes the printer available in RDP sessions.

The remaining parameters are used to select the printer driver in ICA and RDP sessions on Windows servers.

- Give the name of the driver under Windows which is to be used.

If it does not feature in the list, it can be specified under **Use User-Defined Windows Driver Name**.

When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the thin client to the printer. An exception is encountered when using the Windows driver in ICA sessions:

Manufacturer: Generic,  
Model: Generic PostScript  
(Citrix Universal Printer Driver Postscript)

In this case, the print data are prepared on the thin client with the help of the printer driver defined above under **Printers** for the printer model. This requires thin client resources depending on the size of the print job.

## IPP printer sharing

The IPP (Internet Printing Protocol) offers the following configuration options:

<b>Network or host for sharing local printers</b>	Allows printing on the local device from either the local or the global network.
<b>Enable IPP printer browsing</b>	Allows you to search for shared printers in the local or global network and show your shared printers within the network. A shared printer is visible within the network but it may not be possible to print from the network if you do not have the necessary authorization.

### 10.1.2. LPD - Line Printer Daemon

Menu path: **Setup > Devices > Printer > LPD**

LPD printers are used by the BSD printing system and are also supported by Windows servers.

Enable LPD print server	Makes the thin client an LPD print server. The CUPS printers defined under 11.2.1.1 can be addressed under their printer name as a queue name via the LPD protocol.
Print data conversion	Attempts to automatically recognize whether or not the print data need to be prepared by the local printer driver. The <b>None</b> option always forwards the print data unchanged to the printer.
Max. simultaneous connections	Limits the number of print jobs that can be accepted at the same time.
Restrict LPD access	Specifies the sub-networks or hosts from which print jobs can be accepted.

### 10.1.3. TCP/IP

Menu path: **Setup > Devices > Printer > TCP/IP**

You can assign printers connected to your device to a TCP/IP port. The LPT1 (TCP/IP port 3003) is enabled by default. The printer can be connected to one of the following connections, provided that they are available on the device:

- Serial connection (COM 1 or COM 2)
- Parallel connection (LPT 1)
- USB (USBLP 1)
- Additional serial connections: USB adapter or Perle expansion card

Data are forwarded bidirectionally at serial interfaces. This means that other serial devices such as barcode scanners or scales can be operated too.

### 10.1.4. ThinPrint

Menu path: **Setup > Devices > Printer > ThinPrint**

**ThinPrint** allows the bandwidth provided for the transfer of print jobs to be reduced depending on the resources available. The **ThinPrint** client prints either on printers connected to a local interface (serial, parallel or USB), on an LPD network printer or on a CUPS printer defined on the thin client.

The following parameters can be found on the **ThinPrint** setup page:

Port number	Specify the port number via which the ThinPrint daemon is to communicate. Make sure that the port number on the ThinPrint client and the ThinPrint server is the same (communication will otherwise not be possible).
Bandwidth	Enter a bandwidth value (in bits per second) which is lower than or equal to the value specified on the ThinPrint server. A higher value, the disabling of client control or no entry at all means that the ThinPrint server values will be used.
Waiting time between print attempts	Maximum waiting time (in seconds) if a printer is unavailable
Number of print attempts	Number of attempts to contact a printer in order to start a print job.

The list of **ThinPrint** printers is shown on the **Printer** page.

➤ Here you can manage printer configurations by adding, editing or deleting printers.

The page provides an overview of pre-configured **ThinPrint** printers:

Active	Indicates whether or not the printer is visible.
Name of the printer	Name under which the printer can be addressed.
Printer class	Name of the printer class - optional, max. 7 characters without spaces
Device	<p>The following options are available here:</p> <ul style="list-style-type: none"> <li>• + /dev/ttyS0, /dev/ttyS1, ... serial interface</li> <li>• + /dev/lp0, /dev/lp1, ... parallel interface</li> <li>• + /dev/usb/lp0, /dev/usb/lp1, ... USB printer</li> <li>• + Name of a CUPS printer with LPD network printer connection: ThinPrint client prints via the network to the LPD network printer.</li> <li>• + Name of another CUPS printer: ThinPrint client forwards print jobs to the appropriate printer in the CUPS printing system.</li> </ul>
Standard	Defines the selected device as the standard printer.

## 10.2. USB Storage Devices

Menu path: **Setup > Devices > Storage Devices**

USB storage devices can be configured here.

### 10.2.1. Hotplug storage devices

Menu path: **Setup > Devices > Storage Devices > Storage Hotplug**

In this area, you can set up the connection of hotplug storage devices. These can be USB mass storage devices or MMC card readers for example.

You can change the following settings:


- **Default permission:** Default access permissions for hotplug storage devices.

Possible values:

- **Read/Write**
- **Read only**

- **Enable dynamic client drive mapping.** If this option is enabled, hotplug storage devices are automatically added and removed during ICA sessions and RDP sessions.



Before you mechanically disconnect the hotplug storage device from the thin client, you must remove it safely. To do this, click on  in the taskbar.

If the following warning is shown: **The device is still in use! Do NOT disconnect the device.**, the hotplug storage device must not be removed. Close either the named program or close all open files or directories within a session that are located on the hotplug storage device.

- **Number of storage hotplug devices:** The number of hotplug storage devices that can be used in the session.
- **Private drive letter for storage drives:** If this option is enabled, each hotplug storage device will be assigned an individual drive letter. If this option is disabled, a single drive letter will be generated for all hotplug storage devices and each hotplug storage device will be assigned a sub-directory.
- **Start storage drives with this drive letter:** Letter that is assigned to the first hotplug storage device if automatic drive mapping is enabled. Further hotplug storage devices are assigned the next letter alphabetically.
- **ICA read access to hotplug storage devices:** Specifies whether read access to hotplug storage devices is allowed in an ICA session.



This setting is only effective if **Enable dynamic drive mapping** is disabled.

Possible values:

- **Yes:** Read access is allowed.
  - **No:** Read access is not allowed.
  - **Ask user:** Read access can be allowed on request.
- **ICA write access to storage hotplug devices:** Specifies whether write access to hotplug storage devices is allowed in an ICA session.



This setting is only effective if **Enable dynamic drive mapping** is disabled.

Possible values:

- **Yes:** Write access is allowed.
  - **No:** Write access is not allowed.
  - **Ask user:** Write access can be allowed on request.
- **Use storage hotplug beep:** If this option is enabled, a signal tone will be heard when connecting and disconnecting hotplug storage devices.
  - **Show storage hotplug message:** If this option is enabled, hotplug messages will be shown when connecting and disconnecting hotplug storage devices.
  - **Message timeout:** Period of time after which the window with the hotplug messages is hidden. If the time period is set to 0, the window will be shown until it is closed manually.
- ➡ Further settings options can be found under *Drive Mapping (Citrix)* (page 28), *Drive Mapping (RDP)* (page 45) and *USB Access Control* (page 167).

### 10.2.2. Automount Devices

Menu path: **Setup > Devices > Storage Devices > Automount**

Here you can define the devices which are to be mounted automatically when accessed:

List of automount devices	Overview of the automount devices - The most commonly used devices such as the disk drive, CD-ROM etc. are pre-configured.
Edit	Opens and enables one of the pre-defined devices
Add	Manual configuration of devices not pre-defined in the automount device list .
Name	Name given to a device - This name is also used for the sub-directory created in <code>/autofs/</code> .
Device	Allows you to select a suitable device synonym - This can also be entered manually.
File system type	Definition of the file system - The <b>auto</b> option should normally be used. If, however, you use <b>ext2</b> or a problem occurs, you should clearly indicate the file system that you use.
Automount time-out	Regulates the time-out period - Specify in seconds how long the system should wait before the devices accessed are unmounted. The time period ranges from 0 to 600 seconds (10 minutes).



Do not set the time-out period to zero! This may result in data loss.

## 10.3. Smartcard

Menu path: **Setup > Devices > Smartcard**

PC/SC is a service which makes smartcard readers and inserted smartcards available to application programs. RDP and ICA connections make it possible to provide server-side applications with client-side smartcard readers and smartcards. Local applications, e.g. browsers, can also use smartcards in the readers. For these functions to work, the PC/SC daemon must be enabled.

➤ Click on **Enable PC/SC Daemon** to use the PC/SC interface on the thin client.

The **PC/SC Devices Currently Active** window shows the smartcard readers which are currently available. Optional internal readers and a variety of USB smartcard readers are also supported.

## 10.4. USB access control

Menu path: **Setup > Devices > USB Access Control**

You can allow and prohibit the use of USB devices on your thin client. Specific rules for individual devices or device classes are possible.


To enable **USB access control**, proceed as follows:

1. Enable the option **Enable**.
2. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.

3. Create one or more rules for classes of devices or individual devices.

To create a **Class Rule**, proceed as follows:



1. To create a new rule, click  in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Class ID**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Mass Storage**.
4. Under **Subclass**, select the subclass for which the rule should apply or **All [device class]** for all subclasses.
5. Under **Name**, give a name for the rule.
6. Click **OK** or **Cancel**.


The rule is active.

To create a **Device Rule**, proceed as follows:



When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **Uuid** must be given.



1. To create a new rule, click  in the **Device Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.
5. Give the **Device Uuid** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.

Possible values:

- **Global setting:** The default setting for hotplug storage devices is used; see **Default Permission** parameter under *Hotplug Storage Devices* (page 165).
- **Read only**
- **Read/Write**

7. Under **Name**, give a name for the rule.
8. Click on **Next**.
9. Click on **Ok** or **Cancel**.

The rule is active.

Example:



- The set rule prohibits the use of USB devices on the thin client.
- A class rule allows the use of all entry devices (HID = Human Interface Devices).
- A device rule allows the use of the USB storage device with the UUID `67FC-FDC6`.
- The use of all other USB devices, for example storage devices or printers, is prohibited.

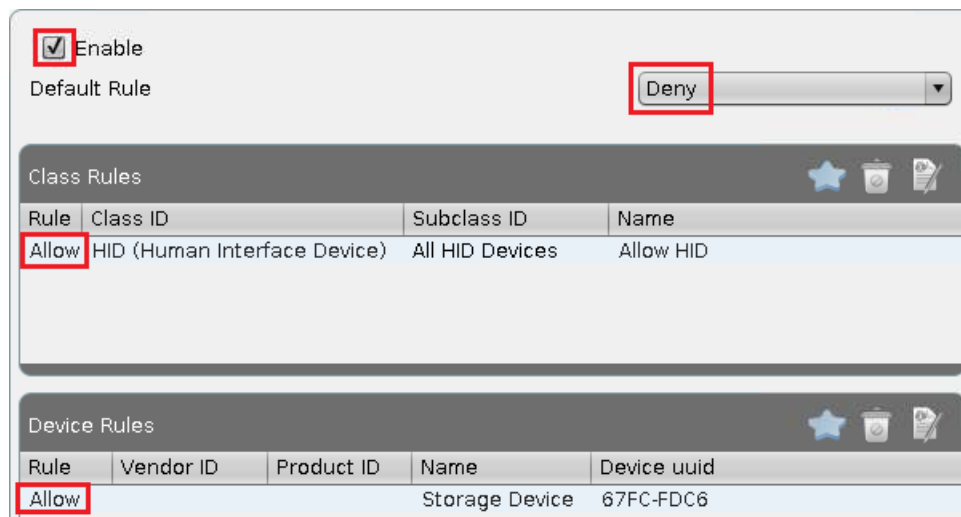


Figure 108: USB access control

➡ Further settings can be found under *Storage Hotplug* (page 165).

## 11. Security

Menu path: **Setup > Devices > Security**

In order to prevent unauthorized access to the thin client setup which could allow deeper penetration into your network, it is essential that you set up an administrator password following the initial configuration.

- You can also use an additional user password which offers various options for permitting restricted configuration by users.

### 11.1. Password

Menu path: **Setup > Devices > Security > Password**

- Under **Password**, set up an administrator password and a user password.

## Administrator and user password

Sets passwords for the administrator and user accounts. The setup will be protected by the administrator password unless the user has been granted access to specific areas.



By enabling this password, the IGEL setup, shell access to Xterm and access to the console will be restricted to the administrator. The **Reset to Factory Defaults** option may only be used with this password. If the setup is locked by an administrator password single setup pages can be enabled for the user - see *Enable Setup Pages for Use* (page 21)r.

## Remote user password

Sets a password for the remote session user (SSH).

## Setup user

Allows the user to access the local setup.



When you enter a password, ensure that the correct keyboard layout is enabled. After all, you will only see stars instead of characters when entering the password and will not be able to see why the password was not accepted.

## 11.2. Login Options

Menu path: **Setup > Devices > Security > Logon**

- Here you can configure the local login procedure for the thin client. You can login via the IGEL smartcard or via the Kerberos protocol, e.g. in a Windows domain.

### 11.2.1. IGEL Smartcard

Menu path: **Setup > Devices > Security > Logon > IGEL Smartcard**

Logging in with IGEL smartcard	Enables local login to the thin client with the IGEL smartcard. Sessions stored on the smartcard become available. The thin client is locked without the smartcard and optional password.
Enable IGEL smartcard without locking the desktop	Enables sessions stored on the smartcard after entering an optional password. The thin client is not locked – even without a smartcard.
Company key	Shared key for smartcards and thin clients. For more details see <i>smartcard personalization</i> (page 112).

You can use the optional IGEL smartcard for local authentication and personalized session configuration ("Flying Doctor Scenario").



Figure 109: IGEL Smartcard

The procedure when using the IGEL smartcard with the internal card reader or an external reading device (USB) is as follows:

1. Enable the IGEL smartcard solution under **Security** → **Login** → **Smartcard** in the setup application.
2. Enter a **company key** to describe your IGEL smartcard.
3. Save your settings before you start personalizing the card.
4. In the **Personalization** window, you can set a login password and add sessions to the card.

Session configurations are stored on the card's IC (integrated circuit) and the session can be used on any IGEL thin client which reads the card.

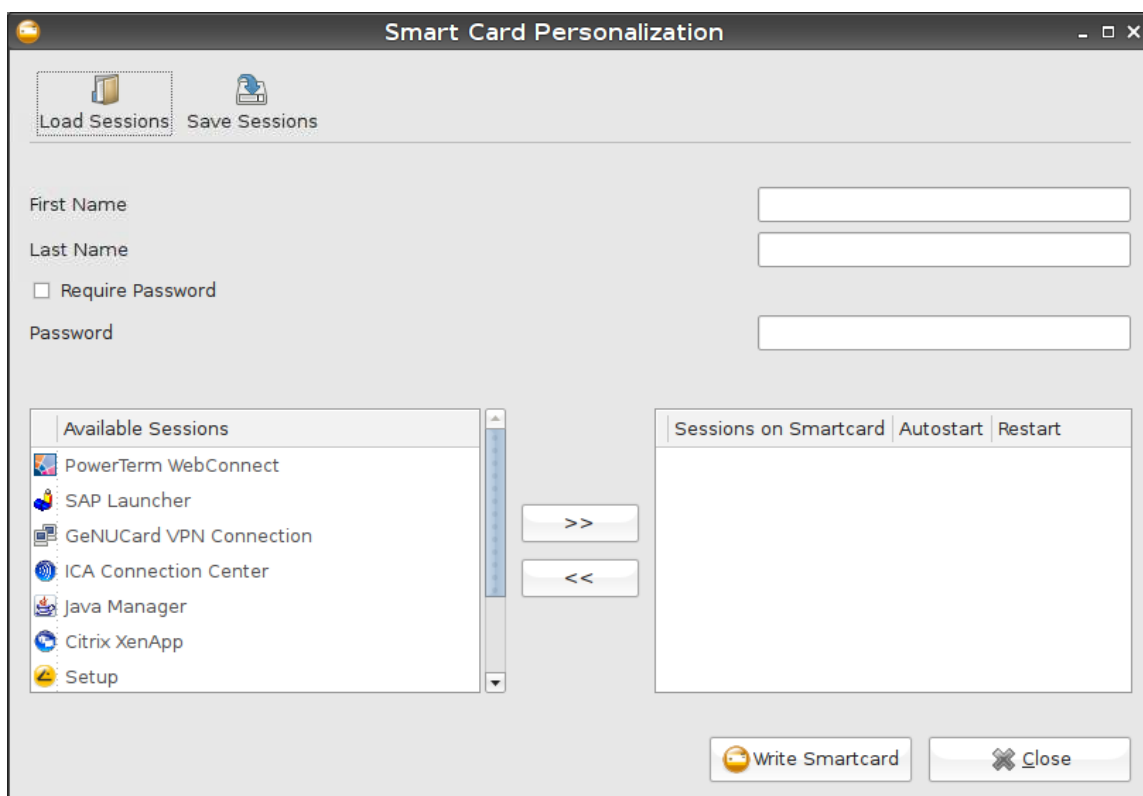


Figure 110: Smartcard personalization

## Company Key

The IGEL smartcard solution also contains a **company key**. This is an additional code which is written to the card and which must match the code of the terminal used. If the two codes do not match, the smartcard cannot be used on that particular terminal. This additional security feature ensures that your terminals cannot be accessed from outside your company. It can also be used within the company in order to restrict employees' access to specific terminals.

## Save User and Password

The procedure for saving users and passwords for authentication is as follows:

- Enter the first name and surname of the user.

You will then be prompted to enter the password for this name.



If the **Demand Password** option is enabled, a pop-up window will always open when a smartcard is inserted. If the wrong password is entered, access to the terminal will be denied.

If the smartcard is merely used to control access to the terminal, the procedure is as follows:

1. Insert a suitable smartcard.
2. Click on **Write to Card** in order to write the data to the card.
3. Remove the smartcard once the writing operation is complete.

You can now program the next smartcard.

## Save Sessions

Saving sessions on the smartcard

If an employee uses a number of different terminals or the terminals are used by many different employees, it may be a good idea to save the sessions used by an employee on his smartcard instead of on the terminal. In this way, the user only needs to call up the applications he requires in order to perform his duties.

The procedure for saving sessions on the smartcard is as follows:

1. Insert the employee's smartcard into the terminal.  
The applications used by the employee are shown on the terminal.
2. Create the sessions you would like to add to the smartcard on the terminal (including an autostart option and personalization of login information). On addition to the first name/surname of the card user and an optional password, you can also add to the smartcard the sessions shown in the Available Sessions area.
3. Once you have added all the required sessions, click on **Write to Card** in order to save the data on the smartcard.

## Test Smartcard

- Test the card you have created.

After performing a warm start and inserting the smartcard, the sessions will be shown immediately on the desktop. Every session which is set to start automatically when you insert the smartcard will be launched.

### 11.2.2. AD/Kerberos

Menu path: **Setup > Devices > Security > Logon > Active Directory / Kerberos**

These setup pages allow you to enable local login to the thin client via the Kerberos protocol.

➡ AD/Kerberos must also be *configured* (page 174) for this purpose.



The login can be used for single sign-on in a number of session types (ICA, RDP).

- **Login to Active Directory Domain:** Connects the login method with the Active Directory.
- **Login methods:**
  - **Explicit:** Expects login with username and password.
  - **Remember last user name:** Initializes the login mask with the username of the last user. Therefore the option **Explicit** has to be enabled.
  - **Smartcard:** Expects login with smartcard.



Select the type of smartcard under **Active Directory / Kerberos > Smartcard** and decide which **Smartcard Removal Action** shall be executed.

- **Logoff shortcut locations:** Allows you to configure the way(s) in which the user can log off.

### 11.2.3. Auto Logoff

Menu path: **Setup > Devices > Security > Logon > Auto Logoff**

Define an **Auto Logoff** action which is carried out when you end the last instance of a session type:

1. Bring up the **Security→Login→Auto Logoff** setup page.
2. Choose a **Session Type**.
3. Choose a **command (Auto Logoff Command)**.
4. Save your settings by clicking on **Apply** or **OK**.

If the last session instance of the selected type is ended, the system will carry out the set action.



The **Shutdown** command carries out the set action. You can check this under **System > Energy > Shutdown**.



The **Logout** command has no effect if you have not defined a login method under **Security > Login** (smartcard, active directory/Kerberos or IGEL Shared Workplace). The **Logoff** command cannot be used together with an appliance - in this case, only the **Shutdown/Suspend** and **Reboot** commands will work correctly.



If you use Auto Logout commands in an appliance, ensure that the appropriate session type was selected - e.g. Horizon when using the VMware Horizon Appliance.

## 11.3. AD/Kerberos Configuration

Menu path: **Setup > Devices > Security > Active Directory / Kerberos**

- Enable and configure Kerberos on these setup pages in order to use this service for login and single sign-on purposes.

<b>Standard realm</b>	Specifies the standard Kerberos realm for the client. Set this value so that it corresponds to your Kerberos realm (Windows domain).
<b>DNS look-up KDC</b>	Specifies whether DNS SRV records should be used to find key distribution centers (KDCs, domain controllers) and other servers for a realm if they are not indicated.
<b>DNS look-up realm</b>	Specifies whether DNS TXT records should be used to determine the Kerberos realm of a host.
<b>No addresses</b>	If this option is set, the first Kerberos ticket is addressless. This may be necessary if the client is located behind an NAT device (Network Address Translation).

### 11.3.1. Realm 1-4

Menu path: **Setup > Devices > Security > Active Directory / Kerberos > Realm [1-4]**

Up to 4 realms where a login is possible can be configured here.

<b>Realm</b>	The name of the realm/the domains where you would like to authenticate yourself.
<b>KDC list</b>	IP or FQDN list of the key distribution centers (domain controllers) for this realm. An optional port number preceded by a colon can be attached to the host name.

### 11.3.2. Domain-Realm Mapping

Menu path: **Setup > Devices > Security > Active Directory / Kerberos > Domain Realm Mapping**

**Domain Realm Mapping** offers translation of a host name into the Kerberos realm name for the services provided by this host.

Standard domain-realm mapping	This should be enabled if the DNS and realm names match. Otherwise, you will need to create user-specific entries in the list.
DNS host or domain name	The entry can be a host name or a domain name. Domain names are indicated by a preceding dot. Host names and domain names should be entered in lower-case letters.
Realm	Kerberos realm name for this host or this domain

## 12. System Settings

Menu path: **Setup > System**

As previously explained under *Quick installation* (page 11), various basic system settings can be configured in the sub-structure.

### 12.1. Time and Date

Menu path: **Setup > System > Time and Date**

1. Go to **System > Time and Date**

The screenshot shows a 'Time and Date Configuration' window. It has two sections. The top section has 'Timezone Continent/Area' set to 'General' and 'Location' set to 'UTC'. The bottom section has a checkbox for 'Use NTP Time Server' which is unchecked. Below it is a text field for 'NTP Time Server'. There is also a checkbox for 'Periodically set Time via NTP' which is unchecked, and a dropdown for 'NTP Update Interval' set to 'daily'. At the bottom left is a button labeled 'Set time and date'.

Figure 111: Time and Date Configuration

2. Maintain your changes.

3. Click Set time and date to save your settings.



You can use a time server within your network (via Network Time Protocol (NTP)) to set time and date automatically during system boot and with periodic update. Make sure the time zone is configured correctly. Choose the region from the drop-down-menus .

Make sure the time zone is configured correctly. Choose the region from the drop-down-menus .



Note: If choosing General as Time Zone Area you have to set your GMT time zone (Location) following the POSIX standard (as usual in Linux) - which means you have to invert the offset of your common UTC time zone! (See tool tip for Location as well.) Therefore it is preferable to set the system's time zone by choosing the corresponding area and location instead of defining the GMT offset.

Example for America/New York: In POSIX standard GMT+5 is the time zone 5 hours west of Greenwich and corresponds to UTC-5.

➡ FAQ: Updating Timezone Information (Daylight Saving Time, DST)

## 12.2. Update

Menu path: **Setup > System > Update**

On the **Update** page, a simple dialog for updating your thin client firmware is displayed. The normal procedure for updating your thin client is as follows:

1. Go to [www.myigel.biz](http://www.myigel.biz) and download the desired firmware image from the IGEL server.
2. Unzip the ZIP file (the usual format in which updates are provided).
3. Save all files in the directory provided either on your local FTP/HTTP server or on a drive which is accessible from the client (e.g. a USB stick, NFS share etc.).
4. Configure the necessary settings (see below).
5. Save your changes and click on **Update Firmware**.

The update process will now proceed automatically.



The update procedure cannot be carried out via PPP/ISDN connections. In this case, you should use a local storage medium (USB stick) to provide the update.

The following information must be given before the update can start (the details required vary depending on the protocol chosen):



Protocol	Allows you to select the protocol to be used (FTP, HTTP, HTTPS etc.) from the drop-down list.
Server name and port	Details of the name or IP address of the server used as well as the port that is to be used
Path name on the server	Details of the directory in which you have saved the update files - starting from the root directory
User name	The user account name
Password	The password for this user/this account

## 12.3. Remote management

Menu path: **Setup > System > Remote management**

If the thin client was registered by an IGEL UMS Server, the server address will be shown under **Remote Administration**.

You can also register the thin client from the thin client itself:

1. Open the **Application Launcher**.
2. In the **System** area, launch the **UMS Registration** application.

The screenshot shows a dialog box titled "UMS Registering" with the subtitle "Registering in Universal Management Suite". It contains the following fields and controls:

- Server Address:** A text box containing "igelrmserver".
- Port Number:** A spin box set to "30001".
- Structure Tag:** An empty text box.
- New Hostname:** A text box containing "mickey".
- Login:** A text box containing "admin".
- Password:** A text box with masked characters (dots).
- + Click to select directory:** A checkbox.
- Buttons:** "Register" and "Cancel" buttons at the bottom right.

Figure 112: Remote Administration

3. Enter the **address** and credentials for your UMS Server.



If there is a corresponding DNS entry for the UMS Server, you can leave the default value `igelrmserver` in the address field.

4. Optional: Select a **destination directory** on the server.
5. Optional: Define a **structure tag** in order to register the thin client in accordance with the UMS directory rules.



Structure tags can also be distributed to thin clients via the DHCP option 226 in order to assist with automatic registration and sorting in the UMS Database. When registering on the UMS, a structure tag obtained via DHCP has priority over a tag entered manually.

6. Optional: Allocate a corresponding **New Hostname** under which the client will be registered in the UMS.
7. Click on **Register**.

### 12.3.1. Legacy 'setup.ini' transfer

Menu path: **Setup > System > Remote management > Legacy 'setup.ini' transfer**

You can also set up the thin client by directly transferring the `setup.ini` configuration file:

1. In **System > Remote Administration**, disable the **Allow remote management** option in order to disable the IGEL remote management service.
2. Click on **Transfer the setup.ini configuration file** to load the configuration needed for the thin client directly via DHCP.

The `setup.ini` file will then be administered manually without the graphical setup, e.g. of the IGEL UMS.

Two transfer protocols are available – TFTP and FTP. The corresponding DHCP tags are:

TFTP (disabled by default)	
ID 66	Name or IP of the server
ID 67	File path on the server The <code>setup.ini</code> file will be searched for in <File path>/.

FTP (enabled by default)	
ID 161	Name or IP of the server
ID 162	File path on the server The <code>setup.ini</code> file will be searched for in <File path>/igel/ud/.
ID 184	User name
ID 185	Password



It is recommended that you set the **Disable when updating** option at the same time. This will ensure that the `setup.ini` and the update data are transferred separately.

## 12.4. Buddy Update

Under **Buddy Update**, you can specify your thin client as an update server for other IGEL thin clients. If you use a thin client as an update server, only the FTP protocol can be used to update the firmware. A number of thin clients can be set up as **buddy update** servers within the network.

Thin clients without a specified update server search for available servers during the update. The first update server found then provides the update.

## 12.5. Shadow

Menu path: **Setup > System > Shadow**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the IGEL Remote Manager or another VNC client (e.g. TightVNC) . The options for the VNC functions are as follows:

Ask user for permission	In a number of countries, unannounced mirroring is prohibited by law. Do not disable this option if you are in one of these countries!
Allow entries from remote computer	If this option is enabled, the remote user may make keyboard and mouse entries as if they were the local user.
Use password	Enable this option to set up a password which the remote user must enter before they can begin mirroring.

### 12.5.1. Secure shadowing (VNC with SSL)

The **Secure Shadowing** function improves security when remote maintaining a thin client via VNC at a number of locations:

- **Encryption:** The connection between the shadowing computer and the shadowed thin client is encrypted.

This is independent of the VNC viewer used.

- **Integrity:** Only thin clients in the UMS database can be shadowed.
- **Authorization:** Only authorized persons (UMS administrators with adequate authorizations) can shadow thin clients.

Direct shadowing without logging on to the UMS is not possible.

- **Limiting:** Only the VNC viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.

Direct shadowing of a thin client by another thin client is likewise not permitted.

- **Logging:** Connections established via secure shadowing are recorded in the UMS server log.

In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.



Of course, this is only relevant to thin clients which meet the requirements for secure shadowing and have enabled the corresponding option. Other thin clients can be "freely" shadowed in the familiar manner and, if necessary, secured by requesting a password. If you would like to allow secure shadowing only, you can specify this in Misc Settings in the UMS Administration area.

## Basic principles and requirements

The **Secure Shadowing** option can be enabled subject to the following requirements being met:

- IGEL Universal Desktop Linux or IGEL Universal Desktop OS 2, each from Version 5.03.190 or IGEL Universal Desktop Windows Embedded Standard 7 from Version 3.09.100
- IGEL Universal Management Suite from Version 4.07.100 onwards
- Thin client is registered on the UMS server
- Thin client can communicate with UMS console and UMS server (see below)

Basic technical principles:

Unlike with "normal" shadowing, the connection between the VNC viewer and the VNC server (on the thin client) is not established directly during secure shadowing. Instead, it runs via two proxies – one for the UMS console and one for the VNC server on the thin client. These proxies communicate via an SSL-encrypted channel, while the local communication, e.g. between the VNC viewer application and the UMS proxy, takes place in the conventional unencrypted manner. As a result, a secure connection can also be established with external VNC programs that do not support SSL connections.

The two proxies (UMS console and thin client) communicate with SSL encryption via the same port as the "normal" VNC connection: 5900. As a result, no special rules for firewalls need to be configured in order to perform secure shadowing.

If secure shadowing is active for a thin client (**Setup>System>Shadowing>Secure Shadowing**), the thin client generates a certificate in accordance with the X.509 standard and transfers it to the UMS Server when the system is next started. The UMS server checks subsequent requests for a secure VNC connection using the certificate. The certificate in PEM format can be found in the `/wfs/ca-certs/tc_ca.crt` directory on the thin client. The validity of the certificate can be checked on the (Linux) thin client using the command: `x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt`

```
VNC Certificate file:
    /wfs/ca-certs/tc_ca.crt

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1572055243 (0x5db3a8cb)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=DE, L=Bremen, O=IGEL
    Validity
      Not Before: Jun  6 06:04:50 2014 GMT
      Not After : Jun  6 06:04:50 2037 GMT
    Subject: C=DE, L=Bremen, O=IGEL
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
        00:a4:e4:67:f3:cf:23:90:06:c3:d6
        5e:0e:00:b8:43:14:6d:61:c5:65:ca
        .....
```

Figure 113: Thin client certificate for secure shadowing

If a UMS administrator calls up the **Shadowing** function in the UMS Console for the thin client, the console receives a signed request from the UMS Server which is then passed on to the thin client to be shadowed. This in turn passes on the request to the UMS server which checks the validity of the request using the original certificate. If this check is successful, the console reports that the channel for the connection between the proxies can be established. The UMS proxy on the console connects to the server proxy on the thin client, and the server proxy in turn establishes on the thin client the connection to its VNC server.

Only when these connections have been established does the console call up the VNC viewer which then connects to the console proxy. The VNC client and VNC server are now connected via the two proxies which transfer data with SSL encryption.



Secure shadowing can be enforced independently of the thin client configuration for all thin clients that support this function: **UMS Administration > Misc Settings > Activate Global Secure VNC.**

## Shadow thin clients securely

In order to shadow a thin client securely (with encryption), the administrator must log on to the server via the UMS console. When doing so, it is irrelevant whether a purely local UMS administrator account is used or the user was adopted via an Active Directory for example. As always, however, the UMS administrator must have the right to shadow the object, *see Object-related access rights* (<http://edocs.igel.com/index.htm#2307.htm>).

The thin client to be shadowed is called up in the navigation tree and, as usual, can be executed via **Shadow** in the context menu. The connection window however differs from the dialog for normal VNC shadowing. The IP and port of the thin client to be shadowed cannot be changed, and a password for the connection is not requested – this is superfluous after logging on to the console beforehand.

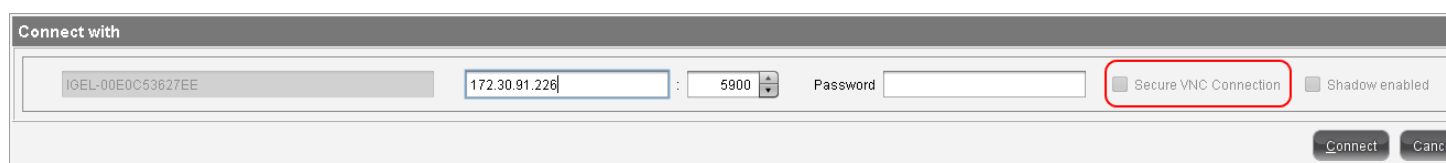


Figure 114: Secure shadowing connection dialog

When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:



Figure 115: Secure VNC connection

## VNC logging

Connections via secure shadowing are always logged in the UMS. Via **UMS Administration>Misc Settings>Secure VNC**, you can configure whether the user name of the person shadowing is to be recorded in the log (the default is inactive).

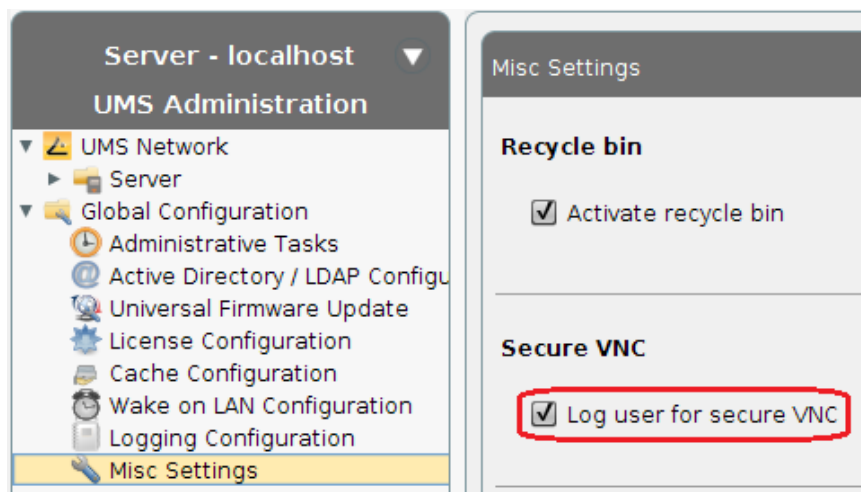


Figure 116: Options for VNC logging

The VNC log can be called up via the **context menu** of a thin client or folder (for several thin clients, **Logging>Secure VNC Logs**). The name, MAC address and IP address of the shadowed thin client, the time and duration of the procedure and, if configured accordingly, the user name of the shadowing UMS administrator are logged.

Secure VNC Logs					
Filter:	<input type="text" value="00E0C56133A9"/>				
Thin Client Name	MAC Address	Thin Client IP	User	VNC Starttime	Duration in sec
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:01:17 PM	98
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:10 PM	32
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:26 PM	19
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:09 PM	44
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:18 PM	39
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:06 PM	48
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:38 PM	20
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:09:24 PM	26

Figure 117: Log entries for secure VNC connections

- To sort the list (e.g. according to user names), click on the relevant column header or filter the content shown by making entries in the **Filter** field.

## 12.6. Remote Access (SSH / RSH)

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

Remote access to the local setup is permitted by default. However, you can restrict remote access to a specific user from a specific host. To enable restriction, give the full name of the host (e.g. `xterm.igel.de`) and the permitted user.

## Power

Menu path: **Setup > System > Power Options**

Under **System > Power Options**, you will find numerous settings for energy management.

System 183

Battery 185

Display 186

Shutdown 187

## 12.6.1. System

Menu path: **Setup > System > Power Options > System**

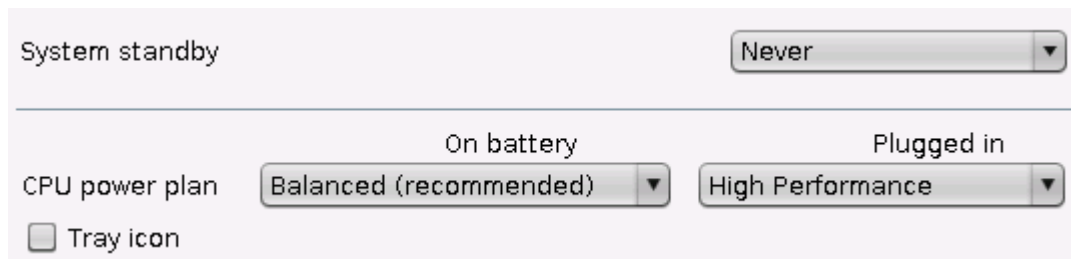


Figure 118: Energy Options System

Standby time	Specify how long the user can be inactive before the system switches to standby mode – from <b>Never</b> or <b>10 Mins</b> to <b>24 Hours</b> .
CPU power plan	<p>Specify here which CPU power plan (CPU Governor) the device is to use in AC mode.</p> <p>Explanation of the settings:</p> <ul style="list-style-type: none"> <li>• <b>High Performance</b>- full performance with maximum processor speed</li> <li>• <b>Balanced (smooth)</b> - slower regulation of performance in a balanced manner according to the demands of programs. Suitable for users who are bothered by the fan frequently running at high speed.</li> <li>• <b>Balanced (recommended)</b> - rapid regulation of performance according to the demands of programs (recommended).</li> <li>• <b>Power Saver</b> - lowest processor speed</li> </ul> <p>The standard settings are <b>High Performance</b> in AC mode and <b>Balanced (recommended)</b> in battery mode.</p>
Tray icon	Enable this setting in order to display a CPU tray icon which allows you to switch quickly between the power plans.



## 12.6.2. Battery

Menu path: **Setup > System > Power Options > Battery**

The screenshot shows the 'Battery' configuration window. It is divided into two main sections: 'Battery Notification' and 'Battery Tray Icon'.  
**Battery Notification**  
 - 'Critical battery level (percentage)': A text input field containing the value '5'.  
 - 'Critical battery action': A dropdown menu with 'Show warning' selected.  
 - 'Critical command': A dropdown menu with 'Shutdown' selected.  
 - 'Low battery level (percentage)': A text input field containing the value '10'.  
 - 'Low battery action': A dropdown menu with 'Show warning' selected.  
 - 'Low command': A dropdown menu with 'Shutdown' selected.  
**Battery Tray Icon**  
 - 'Display percentage': A checkbox that is checked.  
 - 'Display time': An unchecked checkbox.

Figure 119: Energy Options Battery

<b>Critical battery level (percentage)</b>	Here you can configure the battery level percentage below which the battery level is regarded as critical. You can configure two different scenarios.
<b>Critical battery action</b>	Here you can specify what action is to be taken in the event of a critical battery level: <b>No Action</b> , <b>Warning</b> , <b>Execute Command</b> or <b>Execute Command in Console</b> .
<b>Critical command</b>	Enter a valid command here. The standard command <code>user_shutdown -f</code> shuts down the system in the proper manner.
<b>Display percentage</b>	Shows the battery level percentage in the tray.
<b>Display time</b>	Shows the remaining battery running time / charging time in the tray.

### 12.6.3. Display

Menu path: **Setup > System > Power Options > Display**

**Display power management settings**

☒ Handle display power management

	On battery	Plugged in
Standby Time	6 Minutes	10 Minutes
Suspend Time	8 Minutes	12 Minutes
Off Time	10 Minutes	15 Minutes

**Brightness reduction**

	On battery	Plugged in
On inactivity reduce to	20 %	80 %
Reduce after	Never	Never

Figure 120: Energy Options Display

### Set the screen energy options

Handle display power management	Enable this checkbox in order to be able to make the following settings. In older firmware versions, this option was called DPMS (Display Power Management Signaling).
Standby time	Specify how many minutes the user can be inactive before the screen switches to standby mode.
Suspend time	Specify the number of minutes before the screen switches to suspend mode.
Off time	Specify the number of minutes before the screen switches off.

### Brightness reduction

On inactivity, reduce to	Specify to how many percent the screen brightness should be reduced if you are not using the device.
Reduce after	Specify a time between 10 and 120 seconds after which the screen brightness will be reduced.

## 12.6.4. Shutdown

Menu path: **Setup > System > Power Options > Shutdown**

This setup page contains settings for shutting down.

Figure 121: Shutdown

Allow system shutdown	Allows the user to shut down the device.
Allow standby suspend	Allows the user to place the device in standby mode.
Allow canceling of shutdown process	Allows the user to cancel the shutdown or standby process.
Default action	Defines which action is pre-selected in the dialog shown.
Dialog Timeout	Time span in seconds after which the option pre-selected in the dialog is executed.
Disable User Message	When shutting down the device, no dialog which with the user can interact is shown.

## 12.7. Firmware Customization

Menu path: **Setup > System > Firmware Customization**

Configure the firmware to create your own personal workstation.

### 12.7.1. Custom partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

IGEL Linux offers users a data partition on the storage medium. A download/update function which loads data from a server and, where appropriate, updates them can be set up for this dedicated storage area.



If the thin client is reset to the default settings, the custom partition and all data stored on it will be deleted

### Enabling the partition

Menu path: **Setup > System > Firmware Customization > Custom Partition > Partition**

The custom partition is disabled by default.

- Click on **System > Firmware Customization > Custom Partition**, in the setup to enable the custom partition in the IGEL setup for the thin client (or with the IGEL Universal Management Suite) via the setup path.

The size of the partition is shown in the form of a numerical value (bytes) followed by a multiplier.

Sensible figures are for example 100 K (for 100 KiB = 100 \* 1024 bytes) or 100 M (for 100 MiB = 100 \* 1024 \* 1024 bytes).

The screenshot shows the 'Partition' configuration window. At the top, there are icons for a hard drive and a download arrow, with the text 'Partition' and 'Download' below them. A horizontal scrollbar is present. Below the scrollbar, there is a section with a checked checkbox labeled 'Enable Partition'. Under this, there are two input fields: 'Size' containing '92m' and 'Mount Point' containing '/custom'.

Figure 122: Enable Partition



The size of the partition should be set to at least 100 KiB. However, no more than 300 MiB should be reserved for the custom partition (based on the 1 GB standard CF used in IGEL Linux thin clients). This is because subsequent firmware updates may require more storage space than the current version.



Figure 123: Creating Partition

- Click **Apply** or **OK** in order to confirm your settings.

The partition will be created and mounted at the specified location.

A status window provides information on the process and gives details of any errors when creating the partition. If for example there is insufficient space on the storage medium, it will not be possible to create the partition.



Figure 124: Error Message

If you attempt to change the size of a previously created custom partition, you may find that you are unable to do so if a process is still accessing the partition, e.g. if its content is still being shown in the terminal window.

## Defining download source

Menu path: **Setup > System > Firmware Customization > Custom Partition > Download**

In order to load data onto the custom partition, at least one source for partition data must be specified in the Download area.

- Click on **Add**.

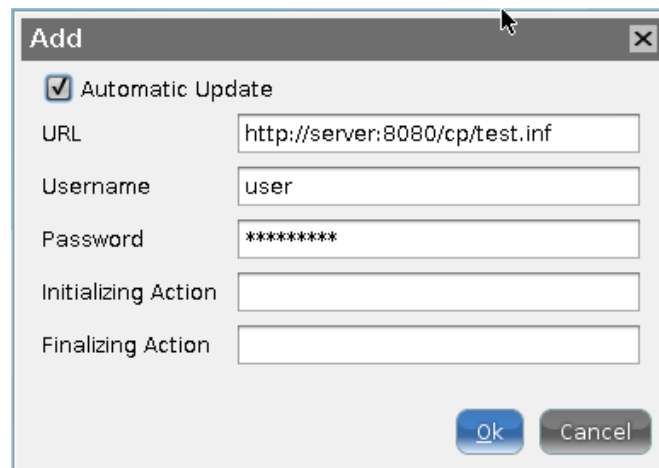


Figure 125: Setting the Download URL.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP, HTTPS, FTP. An `INF` file which in turn references a tar archive zipped using `bzip2` must be given as the target.

The structure of the `INF` file is as follows:

[INFO], [PART]	Header informationen
file="test.tar.bz2"	Zipped tar archive
version="1"	Version of the file

The files to be transferred must therefore be zipped in a `tar` archive which is then compressed using `bzip2`. This file is referenced in the `INF` file which is the target of the URL.

The `tar` archive can be created under Windows, e.g. with the open source program 7-Zip ([www.7-zip.org](http://www.7-zip.org)). This program also allows `bzip2` compression. Under Linux, `tar`- and `bz2`- files can often be created using onboard resources.

The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The Version parameter in the `INF` file must be increased for this purpose.

## Carrying out actions

Menu path: **Setup > System > Firmware Customization > Custom Partition > Download**

Once the custom partition has been mounted or unmounted, commands (Shellscript) can automatically be executed. For example, a program loaded to the partition can be launched or closed upon shutdown (the partition will be unmounted again in the process).

## Example

A custom background image is to be used. The image named `igel.jpg` is zipped into the referenced `test.tar.bz2` file using 7-Zip (see `INF` file above).

The `INF` file and the zipped archive are moved to an IGEL UMS web resource. This can be accessed from the thin client via HTTP.

Make the following settings in the UMS thin client configuration:

1. Enable **Customr Partition** (size e.g. 1 M) and have it mounted on `/custom`.

Under **Download**, a new URL whose target is the `test.inf` file on the UMS server is created:  
`http://[ums-server:9080]/web-ressource/test.inf`

2. Enter the access data for the web server and enable **Automatic Updates** if the image is to be replaced later on.
3. Enter the following copy command as an initialization action in order to copy the unzipped image to the correct location:

```
cp /custom/igel.jpg /usr/share/pixmaps/IGEL_UD_4x3_blue.jpg
```

4. Under **User Interface > Screen > Desktop**, select the entry **Igel blue (4x3)** as the background image.

The associated file will be replaced by your own file.

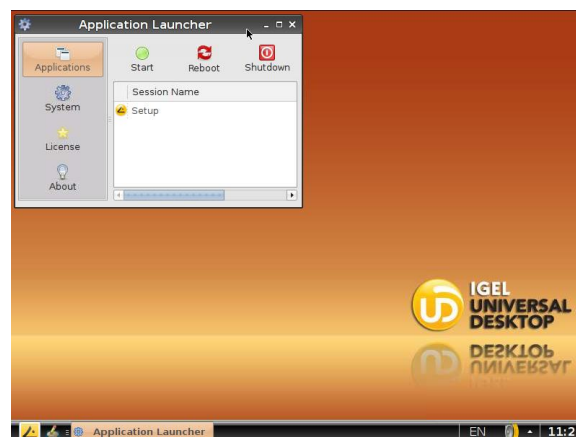


Figure 126: Original background image

5. Save your changes in the IGEL setup and restart the thin client so that it takes the modified settings from the UMS Server.

The custom partition is created and mounted.

The zipped file is transferred, unzipped and copied to the target directory.

The new background image is loaded and displayed:

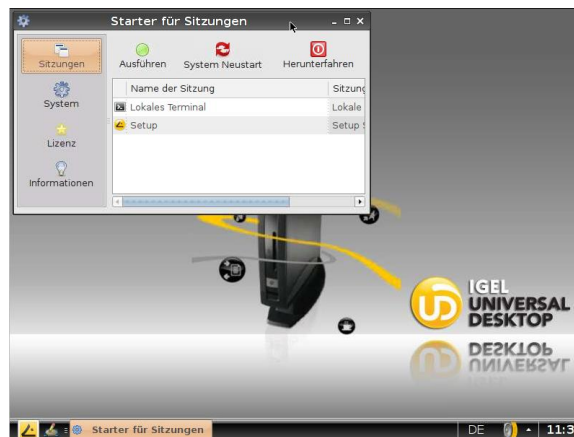


Figure 127: New background image

To replace this image with a new one:

1. Change the JPG in the `test.tar.bz2` file.
2. Increase the version number in the `test.inf` file.

The new version will be downloaded and used then next time you restart the client.



Executable files can also be loaded to the custom partition and called after mounting.

## 12.7.2. Custom Application

Menu path: **Setup > System > Firmware Customization > Custom Application**

Applications which were loaded onto a custom partition for example can be launched via the **Application Launcher** or an icon on the desktop once they have been defined as own applications. In order for this to be possible, a command to call up the application must be entered under **Settings**.

## 12.7.3. Custom commands

Menu path: **Setup > System > Firmware Customization > Custom Commands**

**Custom commands** can be mounted at various points in time during the system start. These commands can use *configured environment variables* (page 198).

## Base commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Base Commands**

**Base commands** run once during the boot procedure. The commands are executed at the following times:



## Initialization

- Not all drivers loaded, not all devices available
- Network scripts not launched, network not available
- Partitions available except firefox profile, scim data, ncp data, custom partition

## Before session configuration

- Not all drivers loaded, not all devices available
- Network scripts launched, network not available
- Partitions available except firefox profile, scim data, ncp data, custom partition
- Sessions not configured

## After session configuration

- All drivers loaded, all devices available
- Network available
- Partitions available except custom partition
- System daemons not launched (CUPS, ThinPrint etc.)
- Sessions configured
- UMS settings retrieved but not effective

## Final initialization command

- All partitions available
- All system daemons launched
- UMS settings effective

## Network commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Network Commands**

**Network commands** run each time the relevant interface (standard `eth0`) starts within the network. The interface can be selected with the `$INTERFACE` environment variables (`eth0`, `eth1`, `wlan0`). The commands are executed at the following times:

## Network initialization

- Network authentication successful (802.1x or WPA)
- No further network settings used

## After network DNS

- Runs after each change in the IP address or host name
- IP address / name server settings used (e.g. via DHCP)

## Before network services

- IP address / name server settings used
- VPN connected (if VPN autostart was enabled in the setup)
- No network / host routing settings used

## Final network command

- Network / host routing settings used
- NFS and SMB drives available
- System time synchronized with time server
- UMS settings retrieved but not effective

## Desktop commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Desktop Commands**

**Desktop commands** run each time the X server starts. The commands are executed at the following times:

## Desktop initialization

- Runs once during the boot procedure
- Desktop environment configured but not launched
- User not logged on (Kerberos, smartcard etc.)

## Before desktop start

- Runs once during the boot procedure
- Desktop environment launched
- Message service launched
- Session D-Bus launched
- User not logged on (Kerberos, smartcard etc.)

## Final desktop command

- Runs after each user logon and desktop restart
- User logged on (Kerberos, smartcard etc.)
- User desktop launched

## Reconfiguration commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Reconfiguration Commands**

**Reconfiguration commands** run when settings are changed via the local setup or the UMS. The commands are executed at the following times:

### After reconfiguration changes

- Runs after an effective change in the thin client settings (local setup, UMS)

## 12.7.4. Corporate design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings allowing you to adapt the user interface to your corporate design are grouped together.

You can place your own logo in the following places:

- *In the bootsplash* (page 195)
- *As a background image* (page 196)
- *As a screensaver* (page 196)
- *As a start button icon* (page 196)
- *As a company logo in the start menu* (page 196)
- *In the taskbar* (page 128)

## Custom bootsplash

Menu path: **Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**

With a bootsplash, you can show your company logo or a specific image during the boot procedure in order to hide the console output from the user.

Requirements: You need to provide an image file for your custom bootsplash on a download server.

Information regarding the image: The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally by changing the position values.

To set up a custom bootsplash, proceed as follows:

1. Enable **Custom Bootsplash**.
2. Specify your download server.



If you have already defined a server for the system update files, you can use the same server settings for downloading the boot image.

3. Configure the following further settings:

- **Custom Bootsplash file:** Give the name of the file that you want to display here.
- **Horizontal/Vertical Position of the bootsplash image:** Give the horizontal and vertical position of the displayed image.
- **Horizontal/Vertical Position of the progress indicator:** Give the horizontal and vertical position of the progress bar.

0 means left-justified, 50 centered and 100 right-justified.

The user-specific bootsplash will be downloaded from the given server if you

- enable **Custom Bootsplash** - see Step 1  
or
- click on **Bootsplash update** if you previously assigned and saved another image during the setup  
or
- you execute a **scheduled Job** in the IGEL Universal Management Suite with the command **Update Desktop Customization**.

## Background

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background**

Decorate the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient, or define your own background image.



You can set up a separate background image for each monitor that is connected to the thin client.

Requirements: You need to provide your own background image on a download server.

Information regarding the image: The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a custom background image. A total storage area of 25 MB is available for all user-specific images.

To set up a custom background image, proceed as follows:

1. Go to Corporate Design > Background (1st Monitor):
2. Enable Custom Wallpaper Download.
3. Give a name for the background image file.
4. Go to Corporate Design > Background (1st Monitor) > Background Image Server.
5. Specify the download server.



If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.

6. Click on Wallpaper Update to download the user-specific background image from the given server.

## Company logos

Menu path: **Setup > System > Firmware Customization > Corporate Design > Company Logos**

Other areas where you can show your company logo in the firmware are the **screensaver** and the **start menu**.

To define an image for the **screensaver**, proceed as follows:

1. Activate **Enable Image display**.
2. Under **Image File/Directory**, give the full path for an image file or a directory containing a number of image files.



If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.

If you do not specify a file of your own, the IGEL logo will be used.

3. Enable **One Image per Monitor** if you would like to see the image (the images) on each individual monitor rather than one image across all monitors.
4. Specify the **image duration** in seconds.
5. Select the **image display mode**:
  - **Small-sized hopping**- small image that jumps across the screen
  - **Medium-sized hopping** - larger image that jumps across the screen
  - **Full screen center cut out** - image is displayed across whole screen, edges can be cut off.
  - **Full screen letterbox** - image is shown in full, with black edge where the format does not match that of the screen.

To define logos for the **start menu**, proceed as follows:

- Under **Start Button Icon**, give the file name of the logo with a full path in order to select your logo as a symbol for the start menu at the bottom left of the taskbar.
- Under **Company logo in start menu**, give the file name of the logo with a full path in order to display your company logo in the start menu window.



In order to see the company logo in the start menu window, you must set the start menu type to **Advanced**. To do this, click on **User Interface > Desktop > Start Menu**.



Figure 128: Start menu

### 12.7.5. Environment variables

Menu path: **Setup > System > Firmware Customization > Environment Variables**

Environment variables allow you to use dynamic parameter content for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session. Within the IGEL Setup, the variables can be found under: **System→Firmware Configuration→Environment Variables**

Pre-defined variables can also be supplied and distributed via the IGEL UMS. Additional defined variables can only be used locally and may be overwritten by a UMS configuration.

The environment variables are available in *Custom Commands* (page 192).

In addition, the following session parameters can be updated with variables:

- ICA - User name (ICA sessions→[Session name]→Logon)
- ICA - Citrix server or Published Application (ICA sessions→[Session name] → Server)
- XenApp - User name (Citrix XenApp/Program Neighborhood→Logon)
- RDP - User name (RDP sessions→[Session name]→Logon)
- RDP - Server (RDP sessions→[Session name]→Server)

#### Use in sessions

1. Enable environment variables under **Enable variable substitution in session**.
2. Specify the variable name and content (e.g. Variable Name = SERVER NAME | Value = test server)
3. Enter the variable name in the session parameter field. The name is preceded by a \$ sign (e.g. \$SERVERNAME )

In the case of RDP and ICA sessions, the setting is implemented after being saved and is entered into the session file. With XenApp, the setting is not implemented until a session starts and is running.

### 12.7.6. Features

Menu path: **Setup > System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Powerterm, Media Player etc. If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will not be shown but will not be deleted either. A disabled session type will not be updated during a firmware update. You should therefore disable unused services in order to speed up update processes.

## 12.8. IGEL System Registry

Menu path: **Setup > System > Firmware Customization > Custom Commands**

You can change virtually every firmware parameter in the Registry. You will find information on the individual items in the tool tips.



However, changes to the thin client configuration via the Registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the thin client is to reset it to the factory defaults!

You can search for setup parameters within the IGEL Registry by clicking on the **Parameter Search** button. If you would like to find the FTP settings for updating the Linux firmware, you can search for the parameter name ftp. The parameter found in the Registry structure is highlighted:

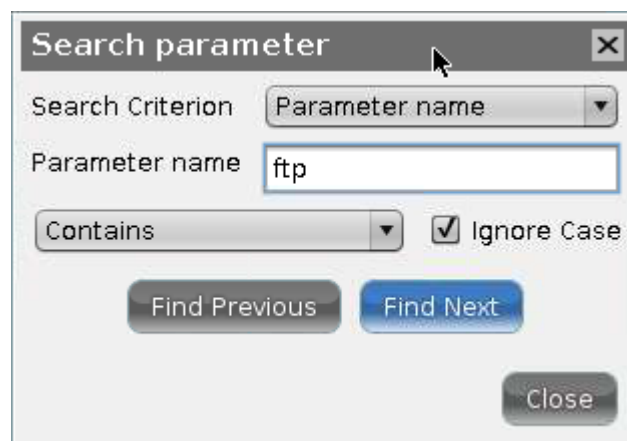


Figure 129: Parameter search in the IGEL Registry

# 13. Index

## A

About this Manual .....	7
Access control.....	123
Accessories .....	101
AD/Kerberos .....	179
AD/Kerberos Configuration .....	180
Address bar.....	88
Advanced .....	88
Advanced Options .....	129
Advanced settings .....	103
Appearance.....	42, 59
Appliance mode.....	69
Application Launcher.....	17, 105
Ask User .....	56
Audio .....	98
Authentication.....	59, 152
Auto Logoff .....	180
Automount Devices .....	173

## B

Background.....	132, 205
Base commands.....	200
Basic principles and requirements .....	186
Battery .....	192
Boot Menu.....	15
Boot Procedure.....	15
Browser Global .....	83
Browser Plugin.....	99
Browser Plug-ins .....	95
Buddy Update .....	185

## C

Carrying out actions.....	198
Certificate .....	163
Certification Authority.....	164
Change Smartcard Password .....	101

Checking the Client Certificate .....	164
Citrix Access Gateway.....	44
Citrix ICA - global settings .....	27
Citrix ICA - Sessions.....	37
Citrix Receiver selection .....	26
Citrix StoreFront / Web Interface .....	41
Codec .....	37
COM Ports.....	48
COM ports - serial connections .....	31
Commands.....	90, 112
Company Key .....	178
Company logos .....	205
Completing the Setup.....	22
Configuration .....	130
Configure connections in the setup.....	158
Configuring Remote Desktop Access .....	55
Connection settings .....	64
Connections .....	58
Contents.....	84
Context menu .....	95
Corporate design .....	204
CUPS - Common UNIX Printing System .....	168
Custom Application .....	200
Custom bootsplash .....	204
Custom commands .....	200
Custom partition.....	196

## D

Data protection.....	86
Defining download source .....	197
Desktop.....	131
Desktop commands .....	202
Desktop integration .....	26, 40
Desktop Integration.....	43
Device Information .....	113
Device support / virtual communication channels .....	32



Device Support / Virtual Communication Channels .....	49
Devices.....	167
DHCP Options .....	160
DigitalPersona authentication .....	33
Disk Utility.....	114
Display .....	193
Display switch .....	102
Display, Keyboard and Mapping.....	53
Domain-Realm Mapping.....	181
Drive mapping .....	30
Drive Mapping .....	47
DriveLock .....	33, 49

## E

Emergency Boot .....	15
Enable setup pages for users.....	24
Enabling the partition.....	196
Encryption.....	89
Energy options.....	121
Environment variables.....	206
Evidian AuthMgr .....	72
Example .....	165, 198
Example configuration for the screen saver.....	139

## F

Failsafe Boot - CRC check.....	16
Features .....	207
Firefox browser.....	82
Firefox Browser Session.....	91
Firewall .....	34, 39
Firmware Customization .....	196
Firmware Update.....	115
Flash Player.....	95
Flash redirection .....	36
Font Services.....	148
Formatting and Meanings .....	7

## G

Gamma correction.....	124
General System Information.....	18
GeNUCard .....	161
GeNUCard Administrator Session.....	162
GeNUCard Options .....	161

## H

Hardware and Network Requirements .....	128
Horizon Client Global .....	60
Horizon Client sessions .....	64
Hosts .....	165
Hotkeys .....	94, 147
Hotplug storage devices .....	171

## I

IBM iSeries Access .....	75
ICA Connection Center .....	101
ICA global options.....	35
Identify Monitors .....	116
IGEL Linux User Manual .....	6
IGEL Smartcard .....	177
IGEL System Registry .....	207
Image viewer .....	117
Important Information .....	2
Individual interface.....	151
Input.....	141
Introduction .....	10

## J

Java Manager .....	111
Java Web Start Session .....	100

## K

Keyboard.....	47
Keyboard / hotkey assignment.....	30
Keyboard and additional keyboard .....	141

## L

LAN interfaces.....	150
Language.....	138

Legacy 'setup.ini' transfer.....	184
Leostream Connection Broker.....	71
License .....	20
Local logon.....	28, 61
Local Logon.....	45
Local Terminal .....	101
Log off.....	43
Logging on and off.....	41
Login Options.....	176
Logoff / Desktop Integration .....	60
Logon .....	38
Look-up.....	114
LPD - Line Printer Daemon .....	169

## M

Magnified view .....	104
Mapping.....	30, 47, 66
Media Player.....	96
Media Player Global .....	97
Media Player Sessions .....	99
Menus and symbol bars .....	92
Monitor Calibration .....	112
Mouse.....	142
Mouse and keyboard.....	65
Multimedia .....	52, 63, 67
Multimedia redirection .....	36

## N

NCP .....	161
Netstat.....	113
Network.....	150
Network commands .....	201
Network Diagnostics.....	112
Network Drives.....	166
Network Information.....	20
Network Integration .....	16
NFS.....	166
NFS Font Service .....	148

NoMachine NX.....	72
Nuance channel for dictation .....	34

## O

OpenVPN .....	160
Options .....	39, 42, 51, 66, 98, 99, 125

## P

Pager.....	136
Parallels 2X client session .....	73
Password.....	176
Password Change.....	43
PDF viewer .....	96
Performance .....	50, 63, 66
Performance and options .....	54
Ping .....	113
Playback.....	97, 99
Power.....	191
PowerTerm selection.....	75
PowerTerm terminal emulation .....	74
PowerTerm WebConnect .....	73
PPTP .....	160
Predefined configuration.....	55
Print .....	85
Printer .....	48
Printers .....	32, 168
Private data.....	86
Protection against tracking.....	87
Proxy.....	67, 85, 167

## Q

Quest vWorkspace Client and AppPortal .....	68
Quick Installation .....	12
Quick Settings Session .....	101
Quick setup.....	24
Quiet Boot.....	15

## R

RDP - global settings .....	44
RDP session.....	52

Realm 1-4.....	181	Smartcard .....	41, 64, 173
Reconfiguration commands .....	203	Smartcard Personalization.....	115
Reconnect.....	39	Soft keyboard.....	111
Reconnect and Refresh.....	43	Softpro SPVC Channel.....	33
RedHat Spice.....	96	Software Requirements.....	127
Remote Access (SSH / RSH) .....	189	Sound .....	50
Remote Desktop Gateway .....	44	Sound Mixer.....	105
Remote desktop web access .....	55	SSH Session .....	80
Remote management.....	183	Start menu .....	137
RemoteFX Support.....	50	Starting the Setup.....	22
Reset to Factory Defaults .....	16	Supported formats and codecs.....	10
Routing .....	165	Systancia AppliDis Client.....	72
<b>S</b>		System .....	191
Save Sessions .....	179	System Information .....	114
Save User and Password.....	178	System Log Viewer.....	105
SCEP .....	164	System Settings.....	182
SCIM (Input Methods) .....	146	System Tools.....	19
Screen .....	120	<b>T</b>	
Screen Saver and Screen Lock .....	138	Tabs.....	83
Screenshot tool.....	109	Taking a screenshot .....	110
Secure shadowing (VNC with SSL) .....	186	Task Manager .....	107
Security.....	88, 176	Taskbar.....	133
Server.....	37, 41, 53	Taskbar background .....	135
Server location.....	27	Taskbar items.....	135
Server options.....	61	TCP/IP .....	169
Sessions .....	18, 26	Test Smartcard.....	179
Setup Application .....	22	The IGEL Linux desktop.....	12
Setup Areas.....	23	ThinLinc.....	76
Setup Search.....	25	ThinLinc Global Optimization .....	78
Setup Session.....	101	ThinLinc Global Options.....	77
Shadow .....	185	ThinLinc Global Server .....	76
Shadow thin clients securely .....	188	ThinLinc Global VNC Optimization.....	79
Shutdown.....	194	ThinLinc Global Window .....	77
Shutdown and Restart.....	21	ThinLinc session user interface.....	80
Signature pad.....	146	ThinPrint .....	170
Simple Certificate Enrollment Protocol - SCEP .....	163	Time and Date.....	182

Touchpad .....	142
Touchpad Advanced .....	144
Touchpad General .....	142
Touchpad scrolling.....	143
Touchscreen .....	145
Touchscreen calibration .....	106
Traceroute .....	114

## U

UMS Registration.....	106
Universal MultiDisplay.....	127
Update .....	183
Upgrade License .....	116
Usage .....	131
USB access control.....	173
USB redirection.....	35, 62
USB Redirection.....	51
USB Storage Devices.....	171
User Interface .....	119
Using the Task Manager .....	108

## V

Verbose Boot .....	15
VERDE session.....	81
Via Browser.....	57
Video.....	98
Virtual Private Network - VPN .....	160
VNC logging .....	188
VNC Viewer.....	81
VoIP Client .....	100

## W

Wake-on-LAN.....	153
Webcam Information .....	117
What is new in 5.08.100? .....	8
Window .....	29, 46, 65, 97
Window settings.....	38, 91
Windows Drive - SMB.....	166
Wireless .....	154

Wireless Manager.....	155
Wireless regulatory domain .....	159
<b>X</b>	
X Session .....	73
XC Font Service .....	148
XDMCP .....	122
X-Server .....	16